



EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA



TECNOLÓGICO
NACIONAL DE MÉXICO

Instituto Tecnológico de Orizaba

DIVISIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN

OPCIÓN I.- TESIS

TRABAJO PROFESIONAL

“MÓDULO PARA LA IDENTIFICACIÓN DE
CIBERBULLYING UTILIZANDO PROCESAMIENTO
DE LENGUAJE NATURAL”

QUE PARA OBTENER EL GRADO DE:
MAESTRA EN SISTEMAS
COMPUTACIONALES

PRESENTA:

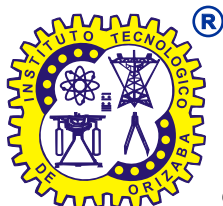
I.S.C. Lissete Rosete Rosas

DIRECTOR DE TESIS:

M.S.C. Luis Ángel Reyes Hernández

CODIRECTOR DE TESIS:

Dra. Laura Angélica Décaro Santiago



ORIZABA, VERACRUZ, MÉXICO.

MAYO 2024



Orizaba, Veracruz, **17/abril/2024**
Dependencia: **División de Estudios de**
Posgrado e Investigación
Asunto: **Autorización de Impresión**
OPCION: I

C. LISSETE ROSETE ROSAS
CANDIDATO A GRADO DE MAESTRO EN:
SISTEMAS COMPUTACIONALES
P R E S E N T E.-

De acuerdo con el Reglamento de Titulación vigente de los Centros de Enseñanza Técnica Superior, dependiente de la Dirección General de Institutos Tecnológicos de la Secretaría de Educación Pública y habiendo cumplido con todas las indicaciones que la Comisión Revisora le hizo respecto a su Trabajo Profesional titulado:

" Módulo para la identificación de cyberbullying utilizando procesamiento de lenguaje natural"

comunico a Usted que este Departamento concede su autorización para que proceda a la impresión del mismo.

ATENTAMENTE

Excelencia en Educación Tecnológica®
CIENCIA – TÉCNICA – CULTURA®

DRA. OFELIA LANDETA ESCAMILLA
JEFA DE LA DIVISIÓN DE ESTUDIOS
DE POSGRADO E INVESTIGACIÓN

OG-13-F06





EDUCACIÓN



TECNOLÓGICO
NACIONAL DE MÉXICO

Instituto Tecnológico de Orizaba
División de Estudios de Posgrado e Investigación

Orizaba, Veracruz, 12/febrero/2024

Asunto: Revisión de trabajo escrito

**C. OFELIA LANDETA ESCAMILLA
ENCARGADA DE LA DIVISIÓN DE ESTUDIOS
DE POSGRADO E INVESTIGACIÓN
P R E S E N T E.-**

Los que suscriben, miembros del jurado, han realizado la revisión de la Tesis del (la) C.

LISSETE ROSETE ROSAS

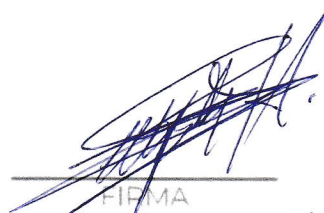
La cual lleva el título de:

Módulo para la identificación de cyberbullying utilizando procesamiento de lenguaje natural

Y concluyen que se acepta.

ATENTAMENTE
Excelencia en Educación Tecnológica®
CIENCIA - TÉCNICA - CULTURAS

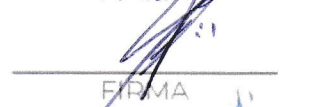
**PRESIDENTE: M.S.C. LUIS ÁNGEL REYES
HERNÁNDEZ**


FIRMA

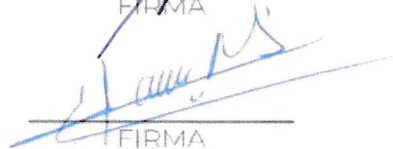
**SECRETARIO: M.C.E. BEATRIZ ALEJANDRA
OLIVARES ZEPAHUA**


FIRMA

VOCAL: M.R.T. IGNACIO LÓPEZ MARTÍNEZ


FIRMA

**VOCAL SUP.: DRA. LAURA ANGÉLICA DÉCARO
SANTIAGO**


FIRMA

TA-09-18



Av. Oriente 9 Núm. 852, Colonia Emiliano Zapata, C.P. 94320 Orizaba, Veracruz.
Tel. 01 (272) 1105360 e-mail: di_orizaba@tecnm.mx | tecnm.mx | orizaba.tecnm.mx



2024
Felipe Carrillo
PUERTO

CARTA DE ORIGINALIDAD

En la ciudad de Orizaba, Veracruz, el día 24 del mes de abril del año 2024, el (la) que suscribe **Lisete Rosete Rosas**, alumno (a) del programa de **Maestría en Sistemas Computacionales** con número de control **M16011208**, manifiesta que es autor (a) del trabajo de tesis titulado "**Módulo para la identificación de cyberbullying utilizando procesamiento de lenguaje natural**" y declara que el trabajo es original, ya que su contenido es producto de su directa contribución intelectual. Todos los datos y las referencias a materiales ya publicados están debidamente identificados con su respectivo crédito e incluidos en las notas bibliográficas y en las citas que se destacan como tal y, en los casos que así lo requieran, se tienen las debidas autorizaciones de quienes poseen los derechos patrimoniales. Por lo tanto, se hace responsable de cualquier litigio o reclamación relacionada con derechos de propiedad intelectual, exonerando de toda responsabilidad al Tecnológico Nacional de México / Instituto Tecnológico de Orizaba.



Lisete Rosete Rosas

CARTA DE CESIÓN DE DERECHOS

En la ciudad de Orizaba, Veracruz, el día 24 del mes de abril del año 2024, el (la) que suscribe **Lisete Rosete Rosas** alumno (a) del programa de **Maestría en Sistemas Computacionales** con número de control **M16011208**, manifiesta que es autor (a) intelectual del trabajo de tesis bajo la dirección del **M.S.C. Luis Ángel Reyes Hernández** y ceden los derechos del trabajo intitulado "**Módulo para la identificación de cyberbullying utilizando procesamiento de lenguaje natural**" al TecNM/Instituto Tecnológico de Orizaba para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y del director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección: msc@orizaba.tecnm.mx . Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.



Lisete Rosete Rosas

Agradecimientos

Agradezco a Dios, quien me ha dado fuerza, sabiduría y perseverancia durante todo este proceso de investigación. Quiero expresar mi sincero agradecimiento a mis padres Verónica y Manuel, así como a mi hermana Gisela, por su amor incondicional, apoyo constante y ánimo inquebrantable, que han sido una fuente inagotable de fortaleza durante todo este proceso. Agradezco sus palabras de aliento, sus consejos sabios y su presencia tranquilizadora en los momentos de duda y dificultad. Su ejemplo de determinación y perseverancia ha sido una inspiración para mí en este viaje académico. Gracias por estar siempre a mi lado, celebrando mis triunfos y compartiendo mis desafíos. Quiero dedicar unas palabras especiales de agradecimiento al amor de mi vida, gracias por estar a mi lado en cada paso del camino, por celebrar mis logros y por ser mi roca en los momentos de adversidad. Aprecio infinitamente tus palabras de ánimo, tus abrazos reconfortantes y tu presencia tranquilizadora durante las largas horas de estudio.

Quiero expresar mi más sincero agradecimiento a todos los profesores y profesoras que me acompañaron durante mi maestría. Sus conocimientos, orientación y dedicación fueron fundamentales en mi formación académica y en el desarrollo de esta tesis. Agradezco especialmente al M.S.C Luis Ángel Reyes Hernández, a la Dra. Laura Angelica Décaro Santiago y al Dr. Asdrúbal López Chau, por su invaluable contribución en áreas específicas de mi investigación. Sus enseñanzas, comentarios y sugerencias han enriquecido enormemente este trabajo. Gracias por su paciencia, su guía y su compromiso con la excelencia académica. Ha sido un honor y un privilegio aprender de ustedes.

Agradezco a mis amigos de la maestría, quienes han sido una parte invaluable de este viaje académico, gracias por estar siempre ahí para mí, por compartir risas, preocupaciones y momentos de inspiración.

Quiero dedicar unas palabras de agradecimiento muy especiales a mis queridos compañeros de cuatro patas. Agradezco sus miradas comprensivas, sus ladridos de ánimo y sus abrazos peludos que siempre han traído luz a mis días más oscuros y tediosos. Gracias por enseñarme sobre el valor del presente, la importancia de la simple alegría y por ser mis fieles compañeros en este viaje. Los amo más de lo que las palabras pueden expresar.

Finalmente, agradezco al Consejo Nacional de Humanidades Ciencias y Tecnologías (CONAHCYT) por el apoyo económico otorgado y al Tecnológico Nacional de México (TecNM) por dar soporte a esta investigación.

Índice general

Índice de Tablas	v
Índice de Figuras.....	vi
Índice de Listados	viii
Resumen.....	ix
Abstract	x
Introducción.....	1
Capítulo 1. Antecedentes	2
1.1. Marco teórico	2
1.1.1. Conducta antisocial.....	2
1.1.2. Resolución de conflictos	2
1.1.3. Perfil psicológico	3
1.1.4. Acoso.....	3
1.1.5. Victimización	3
1.1.6. Victimización por acoso	4
1.1.7. <i>Bullying</i>	4
1.1.8. <i>Cyberbullying</i>	4
1.1.9. Redes sociales.....	7
1.1.10. Servicios web.....	7
1.1.11. Web semántica	8
1.1.12. Marco de descripción de recursos (RDF)	8
1.1.13. Aplicación móvil	8
1.1.14. Aplicación web.....	9
1.2. Situación tecnológica, económica y operativa de la empresa.....	9
1.3. Planteamiento del problema	9
1.4. Objetivo general y específicos	11
1.4.1. Objetivo general.....	11
1.4.2. Objetivos específicos	11
1.5. Justificación.....	12

Capítulo 2. Estado de la práctica.....	13
2.1. Trabajos relacionados.....	13
2.2. Análisis comparativo	25
2.3. Propuesta de solución.....	33
2.3.1. Descripción de la solución	33
2.3.2. Análisis de las tecnologías de información (TI).....	35
2.3.3. Lenguaje de programación	35
2.3.3.1. Java.....	35
2.3.4. Marco de trabajo para el desarrollo de servicios REST	36
2.3.4.1. Jersey	36
2.3.5. IDEs	36
2.3.5.1. NetBeans	36
2.3.5.2. Android Studio	37
2.3.6. Motor de base de datos	37
2.3.6.1. Apache Jena Fuseki	37
2.3.7. Sistema operativo móvil.....	38
2.3.7.1. Android	38
2.3.8. Metodología	38
2.3.8.1. Mobile-D	38
2.3.9. Tecnologías para el procesamiento de lenguaje natural.....	39
2.3.9.1. Apache OpenNLP	39
2.3.9.2. Natural Language Toolkit.....	39
2.3.9.3. CoreNLP	40
2.3.9.4. SparkNLP	40
2.4. Alternativas de solución	40
2.5. Solución propuesta	42
2.5.1. Justificación de la selección seleccionada.....	42
Capítulo 3. Aplicación de la metodología	44
3.1. Cyberbullying: Origen, características, instrumentos y estrategias para la detección del fenómeno.....	44

3.1.1. Origen del ciber acoso	45
3.1.2. Relación del cyberbullying con el bullying tradicional	47
3.1.3. Características del cyberbullying	48
3.1.4. Definición, ¿Qué vamos a entender por cyberbullying?.....	50
3.1.5. Actores del cyberbullying	52
3.1.6. Manifestaciones del cyberbullying	53
3.1.7. Manifestación verbal de violencia entre jóvenes.....	55
3.1.7.1. Tipo de manifestación de violencia verbal	57
3.1.8. Identificación del Cyberbullying a través de instrumentos y medios	59
3.1.9. Bolsa de palabras del lenguaje verbal violento entre jóvenes	65
3.2. Aplicación de la metodología Mobile-D en el desarrollo del módulo de la aplicación móvil.....	71
3.2.1. Exploración	72
3.2.1.1. Establecimiento de los interesados	72
3.2.1.2. Definición del alcance.....	73
3.2.1.3. Requisitos iniciales	75
3.2.2. Inicialización	77
3.2.2.1. Puesta en marcha del proyecto	77
3.2.2.2. Planificación de fases	77
3.2.2.3. Diseño de la aplicación.....	79
3.2.2.4. Diseño de interfaces de usuario	81
3.2.2.5. Diagrama de paquetes	87
3.2.2.6. Diagramas de clases	90
3.2.3. Producción y Estabilización	91
3.2.3.1. Aplicación en Twitter Developer	91
3.2.3.2. Implementación de la conexión con la API de Twitter	93
3.2.3.3. Algoritmo de aprendizaje y clasificación	96
3.2.3.4. Creación de API Python para análisis de tweets	103
3.2.3.5. Métodos de escritura de datos	107
3.2.3.6. Métodos para los servicios web.....	109

3.2.3.7. Pruebas	110
Capítulo 4. Resultados	116
4.1. Valoración del módulo de la aplicación móvil.....	116
4.1.1. Retroalimentación	117
4.2. Monitorización de posibles casos de ciberacoso	119
4.2.1. Resultados de las pruebas	121
4.3. Evaluación y resultados	122
Capítulo 5. Conclusiones y recomendaciones.....	125
5.1. Conclusiones.....	125
5.2. Recomendaciones	125
Bibliografía	127

Índice de Tablas

Tabla 2.1 Análisis comparativo de artículos relacionados.....	25
Tabla 2.2 Comparación de alternativas de solución.....	41
Tabla 2.3 Solución Propuesta	42
Tabla 3.1 Instrumentos de medición de ciberbullying.....	62
Tabla 3.2 Dimensiones de las manifestaciones de ciberbullying.....	65
Tabla 3.3 Ítems clasificados por dimensión.....	66
Tabla 3.4 Requisitos funcionales.....	75
Tabla 3.5 Requisitos no funcionales.....	76
Tabla 3.6 Planificación de fases.....	78
Tabla 3.7 Configuración de hiperparametros a través del método de búsqueda por rejilla.....	101
Tabla 3.8 Desempeño de los clasificadores para la vectorización TF-IDF.....	101
Tabla 3.9 Desempeño de los clasificadores para la vectorización TF-IDF con técnica SMOTE.....	102

Índice de Figuras

Figura 2.1 Patrón arquitectónico MVC aplicado en la aplicación propuesta.....	34
Figura 3.1 Formulario creado en Google Forms.....	67
Figura 3.2 Previsualización de las respuestas obtenidas.....	68
Figura 3.3 Previsualización de la lista de palabras.....	68
Figura 3.4 Representación gráfica de términos más empleados.....	69
Figura 3.5 Nube que contempla todas las dimensiones.....	69
Figura 3.6 Nube de la dimensión "Burla".....	70
Figura 3.7 Nube de la dimensión "Amenaza".....	70
Figura 3.8 Nube de la dimensión "Insulto".....	71
Figura 3.9 Proceso correspondiente a la metodología Mobile-D.....	72
Figura 3.10 Diseño de la arquitectura para el módulo de la aplicación móvil.....	80
Figura 3.11 Casos de uso correspondientes al actor docente.....	80
Figura 3.12 Inicio de carga de la aplicación.....	81
Figura 3.13 Inicio de sesión.....	82
Figura 3.14 Menú principal.....	83
Figura 3.15 Menú principal del módulo de ciberacoso.....	84
Figura 3.16 Listado de alumnos.....	84
Figura 3.17 Gestión de perfil de X.....	85
Figura 3.18 Revisión general.....	86
Figura 3.19 Situaciones de alerta.....	86
Figura 3.20 Dashboard.....	87
Figura 3.21 Diagrama de paquetes del proveedor de servicios web.....	88
Figura 3.22 Diagrama de paquetes del módulo de la aplicación móvil.....	90
Figura 3.23 Diagrama de clases correspondiente al módulo de la aplicación móvil..	91
Figura 3.24 Previsualización del formulario para la creación de aplicación.....	92
Figura 3.25 Credenciales para acceso a la API Twitter v2.....	93
Figura 3.26 Metodología para el análisis de los modelos predictivos.....	97

Figura 3.27 Reglas de clasificación.....	98
Figura 3.28 Interfaces del menú principal de la aplicación y el salón de clases.....	111
Figura 3.29 Interfaz del menú principal del módulo de ciberacoso.....	112
Figura 3.30 Interfaces del listado de alumnos y el registro del perfil de la red social X.	113
Figura 3.31 Interfaz de las situaciones de alerta.	114
Figura 3.32 Interfaces de la sección de dashboard con las estadísticas.....	115
Figura 4.1 Regla añadida al conjunto previo de reglas.	118
Figura 4.2 Conjunto de tweets para su clasificación.	121
Figura 4.3 Alumnos contemplados y el registro del perfil de la red social X.....	121
Figura 4.4 Visualización de tweets negativos y positivos o neutrales.	122
Figura 4.5 Tweets clasificados como negativos.	123
Figura 4.6 Tweets clasificados como neutrales o en calidad de positivos.....	124
Figura 4.7 Estadísticas de la clasificación.	124

Índice de Listados

Listado 3.1 Método "Buscar" a través de username de usuario	94
Listado 3.2 Método general para ejecutar consultas	94
Listado 3.3 Método para obtener los tweets del usuario	96
Listado 3.4 Clase de limpieza de documentos.	103
Listado 3.5 Clase con el modelo predictor	105
Listado 3.6 Ruteo de las solicitudes	106
Listado 3.7 Método para la consulta del username de la red social X correspondiente al alumno.....	107
Listado 3.8 Método para el registro del perfil de la red social X.	108
Listado 3.9 Método para la modificación del perfil de la red social X.	108
Listado 3.10 Método para la lectura de información del username de X.....	109
Listado 3.11 Método para el registro de información del username de X.....	110
Listado 3.12 Método para la actualización de información del username de X.....	110

Resumen

El *cyberbullying*, también conocido como ciber acoso es el tipo de acoso que se presenta a través de dispositivos digitales (celulares, computadoras o *tablets*). A su vez, el ciberacoso ocurre en diversas plataformas como, por ejemplo, las redes sociales, foros o juegos en línea. El objetivo de las personas que cometen *cyberbullying* es atemorizar, enfadar o humillar a otras personas repetidamente durante un tiempo prolongado.

El hecho de que una persona este sufriendo ciberacoso, provoca que se sienta atacado en todas partes, incluyendo su propia residencia. Además, genera consecuencias graves, en las que se ve afectada la salud mental, emocional y física de la víctima. A lo largo de los años se ha apostado por implementar técnicas que prevengan situaciones de ciber acoso, sin embargo, pocas soluciones se encargan de ofrecer una detección temprana de indicios de ciber acoso entre los jóvenes.

Por lo anterior descrito, en el presente proyecto tuvo como objetivo el desarrollo de un módulo para la detección de *cyberbullying* mediante procesamiento de lenguaje natural. Dicho módulo se implementó en una aplicación móvil base que fue desarrollada en el trabajo de tesis “APLICACIÓN MÓVIL DE MONITORIZACIÓN DE BULLYING EN SALONES DE CLASE EMPLEANDO DSM-V Y EL ALGORITMO FOAF” por el maestro en sistemas computacionales, René Navarrete Tenco.

El módulo desarrollado permite identificar posibles situaciones de ciberacoso, a través de la clasificación de tweets pertenecientes a la red social X. Dicha clasificación se logra por medio de técnicas de procesamiento de lenguaje natural y un método de clasificación de aprendizaje supervisado. Así como la aplicación móvil base, el módulo se implementó como una aplicación móvil nativa del sistema operativo Android.

Abstract

Cyberbullying, also known as cyber harassment, is the type of harassment that occurs through digital devices (cell phones, computers or tablets). In turn, cyberbullying occurs on various platforms such as social networks, forums or online games. The goal of people who commit cyberbullying is to frighten, anger, or humiliate other people repeatedly over a long period of time.

The fact that a person is suffering from cyberbullying causes them to feel attacked everywhere, including their own residence. In addition, it generates serious consequences, in which the mental, emotional and physical health of the victim is affected. Over the years, there has been a commitment to implement techniques that prevent situations of cyberbullying, however, few solutions are responsible for offering early detection of signs of cyberbullying among young people.

Due to the above described, the objective of this project was to develop a module for the detection of cyberbullying through natural language processing. This module was implemented in a base mobile application that was developed in the thesis work “APLICACIÓN MÓVIL DE MONITORIZACIÓN DE BULLYING EN SALONES DE CLASE EMPLEANDO DSM-V Y EL ALGORITMO FOAF” by the master in computer systems, René Navarrete Tenco.

The developed module allows identifying possible situations of cyberbullying, through the classification of tweets belonging to the social network X. This classification is achieved through natural language processing techniques and a supervised learning classification method. As well as the base mobile application, the module was implemented as a native mobile application of the Android operating system.

Introducción

En la actualidad la sociedad se encuentra sumergida en una constante evolución tecnológica, donde el Internet y las comunicaciones son los protagonistas. Estos cambios en la sociedad impactan en el contexto social donde los jóvenes o adolescentes se desenvuelven e interactúan; así como existen numerosas ventajas que trae consigo la pequeña brecha entre la tecnología y los adolescentes, también el entorno tiene la preocupante de volverse dañino, pues existen situaciones de riesgo en las que el estado emocional, físico o mental de los adolescentes, se ve afectado. Por otro lado, la violencia y agresión en el sector educativo es un problema persistente alrededor del mundo; ya que regularmente una persona que provoca bullying tradicional hacia una persona, es muy probable que también genere *cyberbullying*, afectando la salud mental de la víctima, lo que la lleva a aislarse de amigos y familiares, tener pensamientos negativos y sentir culpa sobre las cosas que hace o no hace; además es posible dañar la salud física, pues es recurrente que una víctima de *cyberbullying* presente dolores de cabeza, náuseas o dolores de estómago frecuentes. Por lo tanto, en el presente anteproyecto de tesis se propone el desarrollo de un módulo para la detección de *cyberbullying* mediante procesamiento de lenguaje natural. El proyecto propuesto se implementará como un módulo de una aplicación móvil base desarrollada para el sistema operativo Android.

El presente trabajo se encuentra dividió en tres capítulos: en el primer capítulo se presenta el marco teórico, el planteamiento del problema, el objetivo general y específicos, y la justificación; en el capítulo dos se presenta el estado de la práctica y el análisis comparativo; el capítulo tres se describe la propuesta de solución, la descripción de la solución, el análisis de las tecnologías de la información, el cronograma de actividades y los entregables propuestos. Por último, se presentan las conclusiones y referencias del trabajo.

Capítulo 1. Antecedentes

En este capítulo, se describen términos relevantes que conforman este proyecto, las cuales representan la base para el desarrollo del mismo. También se describe la problemática a resolver, el objetivo general y los objetivos específicos a cumplir, así como la justificación de lo que se realizará para dar solución a la problemática planteada.

1.1. Marco teórico

A continuación, se definen algunos términos relacionados con el proyecto de investigación.

1.1.1. Conducta antisocial

Se refiere a la diversidad de actos que violan las normas sociales y los derechos de las demás personas. Una conducta se cataloga como antisocial, dependiendo de la severidad de los actos y de su alejamiento de las pautas normativas impuestas por las leyes y la sociedad, en función de la edad de la persona, el sexo, la clase social y otros factores [1]. Regularmente los actos referenciados a una conducta antisocial son el vandalismo, abusos y agresiones (físicas, sexuales o verbales).

1.1.2. Resolución de conflictos

Se refiere a la forma o método en el que dos o más personas/organizaciones buscan una solución pacífica hacia alguna problemática o disyuntiva presentada. Regularmente el tipo de desacuerdos son emocionales, políticos, financieros, de valores o intereses en común. Según [2] la aptitud para negociar abarca temáticas necesarias para emprender la tarea de abordaje y resolución de conflictos.

1.1.3. Perfil psicológico

Es el conjunto de aptitudes, rasgos y comportamientos psicológicos que definen a una persona y que hacen la diferencia hacia con otros individuos. El perfil psicológico involucra diversos factores de una persona, tales como su forma de comportarse y sentir empatía por los demás, su emotividad, su impulsividad ante diversas situaciones y el carácter que presenta, ya sea sensible o agresivo, así como también su grado de reflexión y el estilo de vida en general. Existen diversos factores que se estudian sobre una persona, dependiendo del tipo de estudio y para la situación que sea requerido un perfil psicológico, por ejemplo, en el caso del *bullying/cyberbullying*, según [3] estudios indican que el agresor regularmente muestra alta tendencia al psicoticismo y por otro lado, las víctimas alta tendencia a la introversión y a la baja autoestima.

1.1.4. Acoso

El acto de acoso (también denominado intimidación) se caracteriza por ser un comportamiento agresivo, repetitivo, metódico y sistemático, que se produce hacia una o muchas víctimas, durante un período de tiempo prolongado. Su principal objetivo es intimidar, insultar, tiranizar, aislar, amenazar y someter emocional e intelectualmente a la víctima [4]. El acoso se somete directa o indirectamente, pues la víctima frecuentemente es controlada por medio de pensamientos o insinuaciones que fácilmente pasan desapercibidas.

1.1.5. Victimización

La victimización se presenta cuando una persona se convierte en víctima de un acto que se provoca hacia sí misma o hacia sus bienes. Por consiguiente, la victimización se encuentra asociada con delitos de infracción sufridos y/o cometidos por otros individuos [5]. Una persona es victimizada en el momento que se comete alguna violación hacia sus derechos; en muchas ocasiones la víctima denuncia estas

acciones cometidas hacia su persona, ante alguna institución que solucione la problemática o sancione a quien/quienes infligieron acciones maliciosas.

1.1.6. Victimización por acoso

Diversas fuentes difieren en cuanto al momento de declarar que una persona sufre de victimización, pues consideran a aquellos individuos que han sufrido la victimización en por lo menos una ocasión; mientras que otros recogen datos sólo de aquellos que son víctimas de acoso frecuente [6]. A medida que el acoso va incrementando o se intensifica, se llega a una victimización más grave, con daños más severos hacia la persona afectada.

1.1.7. *Bullying*

Regularmente se define como un acto o comportamiento agresivo e intencional, que un individuo o grupo comete repetida y consistentemente contra una víctima que no tiene altas capacidades de defenderse fácilmente [7]. Este tipo de agresiones suele presentarse de diferentes maneras en niños y adolescentes, por ejemplo, una manera directa de *bullying* son los abusos físicos y verbales contra una víctima/as (como golpes, patadas, empujones, daños a la propiedad, robo, entre otras) y la exclusión de grupos es un ejemplo de *bullying* indirecto, así como también la calumnia o traiciones.

1.1.8. *Cyberbullying*

El ciberacoso (*cyberbullying* en inglés) es el tipo de *bullying* que se hace presente en medios digitales por medio de algún dispositivo electrónico, como computadoras o teléfonos celulares, por mencionar algunos. Actualmente este fenómeno es más común dentro de las comunidades adolescentes, pues gracias al auge de la tecnología y el uso de las redes sociales, los agresores tienen más accesibilidad a cometer actos maliciosos, tales como el envío de amenazas por medio de mensajes, insultos por medio de comentarios públicos, la publicación de fotografías vergonzosas sin el

consentimiento de la persona implicada, entre otros casos. Básicamente, se refiere a casos en los que los adolescentes usan la tecnología para intimidar, amenazar, humillar o acosar a sus compañeros [8]. Dentro de los tipos de ciberbullying más comunes se encuentran los siguientes:

- *Doxing*: se refiere a la divulgación de información personal o sensible de una persona sin el consentimiento de la misma, con el fin de provocar algún daño o humillación. El doxing está motivado por razones personales, competitivas y políticas que se aplican a usuarios de todas las edades, géneros y experiencia en Internet [9].
- *Fraping*: existen otras formas de ciberacoso como el *fraping*, la creación de perfiles falsos, es una forma peligrosa de ciberacoso en la que un acosador se hace pasar por una víctima y publica en su nombre [10]. El perpetrador usa el nombre, fotos o información personal de la víctima para crear algún perfil falso en las redes sociales, con la finalidad de publicar contenido inapropiado que daña la reputación de la persona en cuestión.
- *Trolling*: ocurre cuando se busca molestar intencionalmente a una persona, por medio de comentarios en redes sociales o videojuegos, donde es más accesible que el perpetrador quede en el anonimato ya que regularmente el sujeto no está relacionado personalmente con la víctima.
- *Flaming*: se refiere a la comunicación hostil, enojada y violenta, que a menudo es un ataque personal ofensivo. Ocurre en una variedad de entornos, como foros en línea y paneles de discusión, salas de chat, correo electrónico y mensajería instantánea [11]. Este tipo de *ciberbullying* incluso tiene un alcance en los chats presentes en videojuegos, donde los usuarios se suelen encontrar en repetidas ocasiones. Es comúnmente identificable que el tipo de mensajes se encuentren en mayúsculas o con muchos signos de exclamación.
- *Phishing*: este tipo de practica se suele llevar a cabo por medio del correo electrónico, donde el perpetrador se hace pasar por alguna entidad confiable

con la que la víctima tiene relación, con la finalidad de que la persona afectada haga clic en algún enlace o descargue un archivo y de esta manera el atacante tenga en su poder la cuenta de la víctima, para después llevar a cabo alguna acción maliciosa y desencadenar otro tipo de *ciberbullying*.

- *Harrasment* (acoso): hace referencia al acoso en línea, provocado por una serie de mensajes hirientes o abusivos hacia una víctima, también suele ser el caso de la insistencia a ser contactada por una persona o un grupo de personas, regularmente a través de redes sociales, mensajes de texto, llamadas o correo electrónico. El acoso por Internet o por teléfono móvil es lo mismo que el acoso por medios más convencionales. El acoso se refiere a acciones hostiles basadas en factores como el género, la raza, la edad o la orientación sexual, de una persona, y es ilegal [11].
- *Sexting*: se refiere al envío de fotos de desnudos o provocativas a través del teléfono celular o Internet [11]. Regularmente estas acciones se llevan a cabo entre dos personas y aunque el *sexting* no es una práctica del *cyberbullying*, suele desencadenarlo al momento de que alguna de las partes comparte las imágenes o las hace públicas, así como los mensajes privados (normalmente de índole sexual explícita) o hace uso de esos recursos para extorsionar a la víctima.
- *Cyberstalking*: la característica más destacada del acoso en línea es la repetición. Generalmente las acciones maliciosas se repiten muchas veces para que sean consideradas acoso cibernético. En algunos casos, las exparejas románticas se convierten en acosadores cibernéticos, envían repetidamente mensajes de texto a la persona en pocos minutos, dejan mensajes de voz en el teléfono celular intentando hacer contacto a través de sitios de redes sociales [11]. El acoso cibernético es similar al acoso que comúnmente se conoce, donde un perpetrador realiza innumerables esfuerzos para tener contacto con la víctima, la diferencia con el acoso normal, es que regularmente el

cyberstalking se da cuando el agresor presenta sentimientos profundos (positivos o negativos) hacia otra persona.

1.1.9. Redes sociales

Las redes sociales, son sistemas que permiten establecer relaciones con otros usuarios [12]. Las redes sociales son sitios o aplicaciones digitales creadas para conectar personas o grupos que tengan relación de acuerdo a intereses, actividades o valores en común, incluyendo relaciones amistosas, de parentesco o profesionales. Regularmente los individuos que se encuentran en alguna red social comparten información, ya sea pública o privada, dependiendo de las configuraciones personales del individuo y de la capacidad de la red social misma para compartir información. Actualmente existen innumerables redes sociales con una diversidad de enfoques, dentro de las más populares se encuentran *Facebook*, *WhatsApp*, *X*, *Telegram*, por mencionar algunos.

1.1.10. Servicios web

Los servicios web son aplicaciones modulares independientes y autodescriptivas que se publican, alojan e invocan a través de una red y tienen un mecanismo estándar para comunicarse con otros tipos de software a través de la red. Los servicios web se consideran integradores, ya que permiten crear una interfaz de usuario capaz de ser usada en aplicaciones, independientemente de sus características de implementación [13]. La mayoría de los servicios web tienen una funcionalidad de solicitud y respuesta, que se logra mediante la conjunción de algunos estándares, por ejemplo, un servicio web simple se compone de cuatro estándares, XML (*Extensible Markup Language*, Lenguaje de Marcado Extensible), SOAP (*Simple Object Access Protocol*, Protocolo de Acceso a Objetos Simples), UDDI (*Universal Description, Discovery, and Integration*, Descripción Universal, Descubrimiento e Integración) y WSDL (*Web Services Description Language*, Lenguaje de Descripción de Servicios Web).

1.1.11. Web semántica

La web semántica deriva de la web y sus bases, dotada de mayor significado, busca que la información sea reunida de forma que la información sea interpretada fácilmente tanto por agentes humanos como por agentes computarizados. Propone implementar descripciones claras del significado de los recursos, para que las propias máquinas comprendan la web lo suficiente como para hacerse cargo del trabajo manual que actualmente realizan los usuarios que navegan e interactúan con la web. La web semántica se centra en: metadatos, ontologías, lógica e inferencia y agentes de software [14].

1.1.12. Marco de descripción de recursos (RDF)

RDF (*Resource Description Framework*, por sus siglas en inglés) es un modelo estándar empleado para el intercambio de información en la web, está especialmente enfocado al significado, por lo tanto, es el fundamento de la *Web Semántica*. Se encuentra conformado por tres elementos fundamentales, los recursos, las propiedades y las declaraciones (también denominadas tripletas). En [15] el marco de descripción de recursos se utiliza para representar información en la Web en forma de tripletas: sujeto-objeto-predicado.

1.1.13. Aplicación móvil

Las aplicaciones móviles son programas que se encuentran dirigidos a ejecutarse en dispositivos móviles, tales como teléfonos celulares o *tablets*. Dichas aplicaciones tienen como finalidad diversas actividades, tanto de ocio como profesionales o informativas. Las aplicaciones móviles se adaptan a las limitaciones de los dispositivos móviles, pero también permiten aprovechar sus capacidades técnicas, como los distintos sensores del dispositivo [16].

1.1.14. Aplicación web

Las aplicaciones web son herramientas que permiten a los usuarios acceder a un servidor web a través de una red utilizando un navegador específico. Por lo tanto, se define como una aplicación a la que se accede a través de la web, ya sea a través de una intranet o de Internet. [17]. Los datos o archivos son procesados y almacenados dentro de la web y gracias a esto no es necesario que se instalen en algún dispositivo, Se basan en una arquitectura cliente-servidor porque combinan secuencias de comandos del lado del servidor para administrar el almacenamiento y recuperar datos con *scripts* del lado del cliente.

1.2. Situación tecnológica, económica y operativa de la empresa

El Instituto Tecnológico de Orizaba es una institución de educación pública superior que pertenece al Tecnológico Nacional de México que reagrupa varios Institutos Tecnológicos Federales y descentralizados en el país. Tiene como objetivo el desarrollo de la ciencia y la tecnología, la formación de recursos humanos y la investigación en estos campos para fortalecer económica y socialmente la región de las altas montañas en el centro del estado de Veracruz. El Instituto Tecnológico de Orizaba se encuentra ubicado en Oriente 9, Emiliano Zapata Sur, C.P. 94320 en la ciudad de Orizaba Veracruz; con teléfono (272) 1105360 y sitio web oficial: www.orizaba.tecnm.mx

1.3. Planteamiento del problema

El acoso y violencia es un problema preocupante. El *bullying* dentro de los salones de clases obliga a replantear la manera de trabajar en el sistema educativo, ya que aspectos familiares, de conducta, gustos, por mencionar algunos, se ve reflejado en el rendimiento académico. Alertar situaciones de riesgo en un salón de clases es el tema a tratar.

Dispositivos inteligentes, el internet y redes sociales se van transformando en un obstáculo para la supervisión ejercida por los adultos, puesto que la brecha digital es muy marcada.

El *cyberbullying*, también conocido como ciberacoso o acoso virtual, es el uso de medios digitales para acosar, intimidar, amenazar o molestar a una persona o grupo de personas a través de ataques personales (ofensas o comentarios hirientes) o la divulgación de información personal o información personal falsa.

Aunque no existe una definición única de ciberacoso, se produce cuando niños, jóvenes o adultos utilizan dispositivos digitales como teléfonos inteligentes o computadoras, redes sociales u otras plataformas digitales para intimidar, amenazar y acosar agresivamente a alguien, generalmente compañeros de clase, compañeros de trabajo o incluso “amigos”.

De acuerdo con un reciente estudio de la firma de ciberseguridad McAfee [18], México tiene un índice de acoso de 41%, cifra que supera el índice promedio mundial, el cual es de 32%. Se estima que el ciber acoso más frecuente se encuentra relacionado con el aspecto físico, a la forma de vestir y al estilo de vida.

La mayoría de los adolescentes que son o han sido víctimas del ciber acoso (alrededor de un 71%) admitieron que ocultan este tipo de situaciones a sus padres y aunque actualmente algunas redes sociales contienen herramientas para reportar comportamientos inadecuados, estas no son utilizadas por pena o vergüenza por parte de los jóvenes.

Existe evidencia de esfuerzos para prevenir el *bullying* y *ciberbullying*, además de acciones para corregir esta grave situación. Mónica Galván Vergara [19] menciona que la gran mayoría de los estudiantes han tenido experiencias respecto al acoso escolar, sin importar el grado ni mucho menos el tipo de escuela.

El desarrollo de aplicaciones móviles, ha ido en constante aumento, pues cada vez existen más aplicaciones que tratan de resolver un problema en la sociedad. Por consiguiente, debido al incremento y perseverancia del cyberbullying es necesario crear herramientas que prevengan o detecten este tipo de situaciones, con la finalidad de disminuir la cantidad de personas afectadas o llevar un seguimiento de personas que se encuentren presenciando ciber acoso. El módulo desarrollado en este proyecto será implementado en una aplicación base desarrollada en el tema “APLICACIÓN MÓVIL DE MONITORIZACIÓN DE BULLYING EN SALONES DE CLASE EMPLEANDO DSM-V Y EL ALGORITMO FOAF” por el egresado de la maestría en sistemas computacionales, René Navarrete Tenco.

1.4. Objetivo general y específicos

En esta sección se plantea el objetivo general y los objetivos específicos del proyecto.

1.4.1. Objetivo general

Desarrollar un módulo para una aplicación móvil base que permita la identificación de *ciberbullying* empleando lenguaje natural.

1.4.2. Objetivos específicos

- Analizar aplicaciones relacionadas con el *ciberbullying* para la determinación del campo de estudio.
- Analizar las variables para la identificación de situaciones de *ciberbullying*.
- Obtener datos relevantes mediante el módulo de la aplicación móvil para su análisis.
- Aplicar el algoritmo de análisis para la identificación de posibles situaciones de *ciberbullying*.
- Implementar el módulo en la aplicación base para analizar datos del caso de estudio.
- Realizar la validación de datos mediante un caso de estudio tomando en cuenta el juicio de expertos en el área.

1.5. Justificación

La problemática presentada crea la necesidad de implementar un módulo de detección de posibles situaciones de *cyberbullying*, pues así como el *bullying* tradicional, el ciberacoso es un fenómeno por el que muchos adolescentes se ven involucrados y afectados; existen soluciones que se basan en prevenir dichas situaciones pero tienen la limitante de solo ser informativas y si es que hay aplicaciones que identifiquen dichos casos, se encuentran destinadas a usarse en un área geográfica específica, diferente a México. El desarrollo del módulo de la aplicación permitirá que se identifiquen situaciones en las que los niños, adolescentes y jóvenes se encuentren en estado de vulnerabilidad con la finalidad de tomar decisiones que atiendan estas situaciones.

Capítulo 2. Estado de la práctica

Actualmente el tema del *cyberbullying* o ciber acoso, es la problemática más común que se presenta en jóvenes o adolescentes; pues la mayoría tienen acceso a dispositivos electrónicos, desde donde están expuestos a ser probables víctimas o agresores. Aunque existe una diversidad de proyectos enfocados en resolver esta problemática usando las TICs (Tecnologías de la Información y la Comunicación) muchos de ellos solo se enfocan en la divulgación de información acerca de lo que es el *bullying/cyberbullying*, brindando información tanto a jóvenes como a padres sobre como detectarlo o prevenirlo; sin embargo, no existen aplicaciones (o se encuentran enfocadas en otras áreas geográficas) que propongan dar una solución y recolecten resultados satisfactorios para detectar casos de ciber acoso. En este capítulo se describe una serie de trabajos que proponen diversas herramientas o información, cuya finalidad es detectar el *bullying* en adolescentes, enfocándose especialmente en el lado del *cyberbullying*. Con los resultados obtenidos de los trabajos descritos, se pretende aportar apoyo en la realización del presente proyecto, permitiendo tener un punto de partida establecido.

2.1. Trabajos relacionados

En [20] se llevó a cabo un estudio cuyo objetivo fue determinar la relación que existe entre la conducta antisocial, la manera en que influye o se ve implicada en situaciones de *bullying/cyberbullying* y las posibles estrategias de resolución de conflictos. El conjunto muestral estuvo constituido por 3026 jóvenes inscritos tanto en instituciones públicas como privadas, con un rango de edad de entre 12 a 18 años, donde un 48.5% era constituido por varones y un 51.5% por mujeres. Para la experimentación se emplearon 4 instrumentos de evaluación psicométrica (3 autoinformes y un cuestionario cumplimentado por los padres), en uno de los instrumentos se evaluó si el adolescente sufrió o provocó *bullying* presencial, *cyberbullying* o la combinación de ambos; determinando que rol presuntamente asumen: víctima, agresor y observador. Como resultado de la aplicación de los diferentes instrumentos se obtuvieron perfiles

psicológicos que presentaban los adolescentes (varones y mujeres), enfatizando en que los jóvenes con un alto índice en conducta antisocial, tenían mayor uso de las estrategias agresivas para la resolución de conflictos y un mayor nivel en las posibilidades de estar implicados en situaciones de *bullying/cyberbullying*; en cualquiera de los roles posibles, víctimas, agresores y observadores.

Ortega [21] llevó a cabo un estudio para analizar las diferencias entre los estudiantes involucrados en situaciones de ciberacoso, las actitudes que presentan y la manera en que participan en conductas escolares violentas, ya sea directas o indirectas. El estudio abarcó una muestra de 1062 estudiantes (con edades entre 12 y 18 años) ubicados en el nivel secundaria, conformado por hombres y mujeres. Se aplicaron 3 instrumentos para la evaluación y obtención de su perfil psicológico, se evaluó la frecuencia en la que una persona participó en conductas agresivas por medio de los medios digitales, las actitudes positivas y negativas hacia la autoridad por parte de los adolescentes; también se hizo uso de una escala de agresión escolar, que evalúa las conductas agresivas hacia los compañeros de clase, contemplando un periodo de los 12 últimos meses. Los resultados arrojaron que casi la mitad de los adolescentes contemplados en la muestra, acosaron a sus compañeros a través de algún medio digital; por lo que el estudio clasificó a los estudiantes en tres grupos diferentes, los no agresores, agresores ocasionales y agresores severos.

Paez [22] examinó la influencia de los factores individuales, de apego y de victimización sobre la probabilidad de ciberacoso, empleando una muestra de 12,642 jóvenes. Se consideraron tres hipótesis, la primera indicó que los factores individuales de los adolescentes influyen en la posibilidad de ciberacoso, la segunda hipótesis planteó que los adolescentes que poseen vínculos negativos o débiles con sus tutores, maestros o compañeros, son más propensos a provocar *cyberbullying*; por último, la tercera hipótesis planteó que los adolescentes que previamente estuvieron involucrados en situaciones de acoso tradicional, tenían más probabilidades de ciberacoso. Mediante una encuesta se recopiló información sobre la

perpetración de ciberacoso contemplando la muestra de adolescentes entre 10 y 17 años. Los resultados arrojaron que la mayoría de los casos de ciberacoso eran precedentes al acoso tradicional y a la presencia de vínculos débiles de los adolescentes con sus padres, maestros o compañeros; pues los adolescentes que tenían una relación buena con su entorno familiar o académico, no presentaron asociaciones con ser ciberacosadores.

Es muy común que se presente una serie de palabras u oraciones que son indicadores de la presencia de ciberacoso en las redes sociales, es por esto que, en [23] se propuso un léxico de ciberacoso para las redes sociales empleando un enfoque ontológico. El enfoque consto de varias fases, las cuales concluyeron en el desarrollo de la ontología de ciberacoso de exclusión, ordenado alfabéticamente y compuesto de 13 palabras clave que van de la mano con su definición y su categoría. Estas palabras se seleccionaron en función a una lista de palabras de vocabulario negativo de *Enchanted Learning*; la definición se obtuvo de *FrameNet* (base de datos léxica en inglés y en línea). El autor propuso que el léxico presentado, tiene la capacidad de ser utilizado como diccionario en las redes sociales para considerar palabras o frases que dirijan su sentido hacia una situación de posible ciberacoso, permitiendo la prevención de este fenómeno.

Noviantho et al. [24] construyó un modelo de clasificación para identificar conversaciones de ciberacosadores, empleando el método de minería de texto *Naive Bayes* y SVM (*Support Vector Machine*, Máquinas de Vector Soporte); se seleccionaron estas técnicas ya que las máquinas de vector soporte demostraron que funcionaban bien en la clasificación de texto de alto sesgo y por otra parte, *Naive Bayes* requiere pocos datos para la parte del entrenamiento y por lo tanto produce resultados máximos. El método de clasificación obtuvo 4 clases con una precisión promedio del 92.81% para *Naive Bayes* y un 97.22% para SVM con un kernel poly; por lo tanto, se concluyó que el modelo más óptimo para separar la muestra en diferentes clases fue SVM con *kernel poly*. La clasificación de las conversaciones analizadas resultó un

tanto difícil porque se suelen usar palabras cortas en las conversaciones de texto, así que se requirió el procesamiento previo de dichas conversaciones para poder implementar el algoritmo de corrección ortográfica.

En [25] se diseñó e implementó un sistema que emplea las publicaciones y los comentarios de los usuarios en la red social *Facebook*, para clasificar dichas publicaciones en alguna de las categorías que se plantearon, contemplando: Crimen, Disturbios, Peor y Vulgar. El análisis se llevó a cabo mediante el algoritmo NLP (*Natural Language Processing*, Procesamiento del Lenguaje Natural) de tal manera que se permita detectar los sentimientos de los usuarios. El propósito de este sistema fue bloquear de inmediato el contenido que no esté moralmente correcto o que sea dañino para los usuarios. Este trabajo concluyó en que con la implementación de este sistema es posible proteger a los niños, adolescentes y jóvenes de los ataques de ciberacoso, pues si se detectan a tiempo las publicaciones o comentarios maliciosos es posible tratar con eficiencia los delitos que se cometen a través de las redes sociales, pues una práctica común es la de adultos que se hacen pasar por adolescentes y pretenden engañar a otros adolescentes con la finalidad de conseguir algún objetivo malicioso, tal como conseguir fotos privadas de índole sexual o incluso preparar al adolescente para cometer un delito presencial, como secuestro.

En el trabajo de Farag [26] se sugirió que también algunas técnicas de aprendizaje no supervisadas y otros enfoques demuestran ser igual de efectivos que las técnicas de aprendizaje supervisadas para detectar el ciber acoso; aplicando técnicas en textos, para la detección de roles, del estado emocional, la anotación automática y los métodos estilométricos. De acuerdo con las investigaciones de [26] se determinó que los métodos distintos a los supervisados empleados para la detección del ciberacoso eran: codificadores automáticos, aprendizaje profundo, semisupervisado, modelado de series temporales y *clustering* (agrupamiento), pues se emplearon en diferentes plataformas, tales como *MySpace*, *X*, *YouTube*, *Formspring*, *ask.fm* e *Instagram* para detectar situaciones de acoso. El resultado de la investigación, demostró que el

método para detectar situaciones de *cyberbullying* depende de la plataforma que se esté analizando. Asimismo, se planteó como trabajo a futuro que la detección de roles ayudaría a revelar al perpetrador; se concluyó que con regularidad el estado emocional de una ciber víctima regularmente la lleva a eliminar desde una foto de perfil, hasta la eliminación de su cuenta en determinada plataforma y en casos más severos daría indicios a través de las redes sociales de un posible suicidio.

En [27] se desarrolló un modelo automatizado para identificar y medir el grado de *cyberbullying* en las redes sociales, además del diseño de una aplicación de *Facebook* que notificaría a los padres en caso de que los adolescentes sean víctimas de ciberacoso, se incluyó un módulo de recuperación de datos, un módulo rastreador de finalización de consultas para el seguimiento de las solicitudes de información asíncronas y paralelas enviadas a *Facebook*; el módulo de identificación de *cyberbullying* empleó los datos recopilados para estimar la probabilidad de que el adolescente fuera víctima de ciberacoso a través de la plataforma *Facebook* utilizando un rango de intimidación que se utiliza para presentar la información más sintetizada y simplificada a los padres, junto con una lista de sitios web o instituciones que ofrezcan ayuda para abordar el caso y prevenir los posibles futuros ciberacosos. La aplicación también cuenta con un componente de señales de advertencia, el cual hace el conteo de la cantidad de contenido hiriente o insultante recibido por el adolescente. Como resultado del proyecto, se obtuvo la aplicación *BullyBlocker*, que identifica si un adolescente se encuentra implicado en una situación de *cyberbullying* y brinda información a los padres del mismo para tomar las medidas adecuadas.

En [28] se realizó un estudio cuyo objetivo principal fue determinar la percepción que los estudiantes tenían sobre el ciberacoso en redes sociales. El espacio muestral para este proyecto fue delimitado a 200 alumnos, a los cuales se les aplicó un cuestionario (escala Likert). Las percepciones que tenían los estudiantes se dividen en cuatro categorías, las percepciones sobre el concepto de ciberacoso, sobre la causa del ciberacoso, las percepciones del castigo dado a los perpetradores de ciberacoso y la

percepción del impacto del ciberacoso en las víctimas. Los resultados arrojaron que más del 50% de los estudiantes piensa que el ciberacoso es la acción de enviar de manera continua, mensajes cortos o mensajes de texto a través de los medios digitales, que sean hirientes o amenazantes. Asimismo, más del 40% de los participantes coincidió en que el ciberacoso comúnmente se produce por venganza, molestia o frustración; el 40% estuvo de acuerdo en que los agresores tendrían que ser orientados por su familia y recibir sanciones severas. De igual forma, se determinó que el 50% de los estudiantes concordó en que lo más recomendable era dar apoyo moral a las víctimas de ciberacoso, para que superen el evento traumático.

Salawu [29] propuso una aplicación móvil (nombrada *BullStop*) diseñada para detectar y prevenir el ciberacoso en las plataformas de redes sociales. Dicha aplicación se integró por una arquitectura en la que se utiliza un modelo de aprendizaje profundo generalizado, empleado para identificar casos de ciberacoso a partir de la información básica del usuario; este modelo es capaz de realizar la clasificación de etiquetas múltiples que acepte datos textuales; el modelo se entrenó para predecir etiquetas de ciberacoso, insultos, blasfemias, sarcasmos, amenazas, discriminación, spam y pornografía. Cuando un usuario instala la aplicación se le pide se registre a la misma y asocie su cuenta con su perfil de alguna red social, dando los permisos requeridos, cuando lleguen nuevos mensajes o comentarios estos serán clasificados de acuerdo al modelo y si son indicios de algún tipo de ciberacoso, se eliminan o se bloquea al remitente temporalmente, permitiendo que los mensajes y personas bloqueadas se revisen en un apartado de la aplicación en dado caso que no sea una situación de riesgo y de esta manera seguir entrenando al modelo. Los resultados fueron satisfactorios ya que las personas que testearon la aplicación dieron visto bueno de la misma y se logró apreciar su correcta funcionalidad, tomando como caso de estudio la red social *Twitter*.

En [30] se diseñó y desarrolló una aplicación móvil (nombrada *#StopBully*) enfocada en mejorar la comprensión de los conceptos de *bullying* y *cyberbullying* entre los

estudiantes a través del entretenimiento educativo. La aplicación se diseñó en Android y proporcionó una página informativa con conceptos y datos significativos en el temario abarcado por el acoso y por el ciberacoso; la aplicación cuenta con un botón de emergencia, el cual comunica al usuario con alguna autoridad capacitada para denunciar algún caso de *bullying/cyberbullying* en el que estuviese involucrado. Los conceptos del ciberacoso se introdujeron por medio de una serie de comics animados, asimismo la plataforma cuenta con juego de entretenimiento educativo que sirve para profundizar los conceptos de *#StopBully*. Se llevo a cabo una prueba en la que participaron 30 estudiantes, en un principio se les aplico una encuesta con la finalidad de obtener la información que estas personas tenían sobre el *bullying* y el *cyberbullying*, después se les dio una breve introducción hacia la aplicación y se les permitió explorarla por sí mismos para adentrarse en las funciones de la misma; al finalizar el tiempo de exploración se les aplico nuevamente un cuestionario y como resultado se obtuvo que hubo una diferencia significativa en el antes y el después de usar la aplicación, demostrando que gracias al uso de la aplicación *#StopBully* se aprendía, mejoraba o pulía de manera concreta los conocimientos de estos grandes fenómenos (*bullying* y *cyberbullying*).

En [31] se realizó un estudio de enfoque lingüístico sobre los mensajes que son intercambiados a través de las redes sociales, específicamente en la aplicación de mensajería anónima *Sarahah*. Para llevar a cabo el análisis en el proyecto, se recopilaron mensajes de *Sarahah* obtenidos utilizando la API de búsqueda de *Twitter*; los mensajes de la aplicación de mensajería anónima se encuentran en forma de imágenes, por lo que se necesitó algún software de reconocimiento óptico de caracteres (perteneciente a *Google*) para extraer la información de dichas imágenes. Esta extracción se dividió en tres componentes, el mensaje de texto como tal, la reacción del usuario al momento de compartir el mensaje en *Twitter* y alguna otra información relevante del perfil del usuario. La cantidad de mensajes recopilados fue de 76278, los cuales conformaron el conjunto de datos; con ayuda de técnicas de

preprocesamiento de lenguaje natural se eliminaron palabras vacías, tokenización y derivación de Porter sobre los mensajes. Se hizo uso de la asignación latente de Dirichlet (empleada para buscar textos similares) con la finalidad de encontrar palabras relacionadas con la intimidación. Se identificaron diferentes tipos de mensajes comúnmente emitidos a través de la aplicación *Sarahah*, clasificándolos en cuatro categorías: confesión, preguntas, opiniones sobre temas mundiales y mensajes de inspiración. Se concluyó que la mayoría de los mensajes de intimidación se encontraban en las categorías de confesión y de preguntas; de igual forma los mensajes de intimidación se clasificaron como sexuales, de odio y de coqueteo inapropiado.

En [32] se propuso dar un seguimiento a la verificación de la eficiencia de *NettOpp*, una aplicación móvil dirigida a adolescentes que estuvieron implicados en una situación de ciberacoso. Dicha aplicación tuvo como objetivos principales, reducir los problemas de salud mental que dejaron las perpetraciones de esta índole en los jóvenes. Asimismo, se buscó elevar la autoestima, su calidad del sueño y, por ende, reducir el ciberacoso. La aplicación móvil constó de dos módulos, el primero fue psicoeducativo, pues incluye información sobre el *cyberbullying*, sus consecuencias, derechos, leyes y consejos prácticos para hacerle frente a un evento de esa índole; el segundo modulo, brindó recursos como ejercicios y técnicas para mejorar la angustia emocional después de haber pasado por una situación difícil. Se obtuvieron resultados satisfactorios con el caso de estudio aplicado a adolescentes de entre 11 y 16 años, donde se notaron estadísticas significativas después de emplear la aplicación en prueba; sin embargo, es un estudio que se llevará por más tiempo con la finalidad de obtener resultados más acertados y verificar que áreas de oportunidad tiene la aplicación o si existen modificaciones importantes en las que trabajar.

En [33] se evaluó la viabilidad y aceptabilidad de IMPACT (Medio de Intervención para Prevenir los Conflictos Cibernéticos a través de la Tecnología) la cual es una intervención remota basada en una aplicación para reducir el efecto del ciberacoso.

En un periodo de tiempo contemplado desde el 30 de enero de 2020 y el 3 de mayo del mismo año, se realizó la difusión de información a través de la red social *Instagram*, de donde se recolectó una muestra de 80 adolescentes con antecedentes de haber presenciado eventos de *cyberbullying*; se les aplicó una encuesta de autoinforme y también una entrevista remota empleando *Google Meet*. Los participantes rondaron entre los 15 años de edad, predominaba el sexo femenino y más de dos tercios de los participantes mencionaron que *Instagram* era su plataforma digital más utilizada. Como resultado se obtuvo que la mayoría de los participantes estaban conformes con IMPACT, pues ayudó con el bienestar de los adolescentes con antecedentes de ciber victimización.

Foong y Oussalah [34] propusieron un sistema online que permitió la detección y el seguimiento de casos de ciberacoso en foros y comunidades en línea; este sistema se conformó por componentes básicos del lenguaje natural, contemplando insultos, amenazas y oraciones escritas en segunda persona. Se hizo uso de un sistema de aprendizaje automático y de ontologías para clasificar la aparición de ese tipo de vocabulario presentes en los documentos del sitio web o del foro, con la finalidad de que se emita un mensaje a la seguridad del sitio y este tome medidas adecuadas o necesarias. Se realizaron las pruebas correspondientes de este sistema en la plataforma digital *Ask.fm* (red social en la que los usuarios realizan preguntas de cualquier índole a otros usuarios, teniendo la posibilidad de preguntar bajo su nombre o de forma anónima), de los datos extraídos el 70% se utilizaron como entrenamiento. Mediante técnicas de minería de datos, se obtuvieron métricas como la exactitud, la precisión, la exhaustividad, medida F1 (precisión y exhaustividad) y F2 (precisión y exhaustividad para un valor beta). Gracias a este trabajo se planteó una apertura a trabajos futuros, empleando el modelo propuesto o incluso mejorándolo de tal forma que se adapte a otro tipo de red social.

El objetivo de [35] fue examinar los métodos existentes de detección del ciberacoso para integrarlos en una aplicación móvil que alerta a los padres en caso de que su hijo

sea una potencial víctima o autor de ciberacoso. La aplicación (desarrollada en *Android Studio* y el lenguaje de programación *Java*) se compuso por dos componentes, el de la aplicación móvil y el componente de aprendizaje automático. El modelo que se empleó para incorporar al aprendizaje automático fue una recolección de datos extraídos de *Twitter*, originalmente fueron 5000 tweets los cuales una vez pasados por filtros para eliminar los tweets no deseados, quedaron un total de 1200; utilizando *Spyder* (IDE para Python) se eliminaron algunos elementos de los textos que no serían de utilidad para la detección del ciberacoso, como espacios en blanco adicionales, números y símbolos. Una vez limpios los datos, se clasificaron empleando técnicas de minería de datos (empleando 25% de datos de prueba) como arboles de decisión, para identificar que mensajes pertenecían a la categoría de ciberacoso y cuáles no. Teniendo como resultado buenas métricas incluidas la precisión, exhaustividad y exactitud que mostraron una eficacia notable del modelo propuesto, se argumentó que la aplicación propuesta cuenta con una GUI (*Graphical User Interface*, Interfaz de Usuario Gráfica) más amigable con los padres de familia en comparación con otras aplicaciones.

En [36] se planteó que siempre se busca prevenir la existencia de un caso de ciberacoso y también detectar los eventos que ya estén ocurriendo para darles una pronta resolución; es por esto que se desarrolla una aplicación denominada MDEG (*Mobile Digital Etiquette Game*, Juego de Etiqueta Digital Móvil) la cual se encarga de capacitar a los niños de nivel primaria a través de preguntas basadas en escenarios propuestos de acuerdo con los intereses de los niños que rondan esas edades; la aplicación constó de tres secciones principales, la sección de aprendizaje o capacitación es donde los niños aprenden sobre lo que es el ciberacoso o el acoso presencial, introduciendo estos temas por medio de escenarios simples que el niño sigue fácilmente, la segunda sección es un examen en la que se ponen en prueba los conocimientos ya adquiridos durante la primera sección. Como ultima sección se encontró la puntuación obtenida de la prueba correspondiente. Los resultados

mostraron que la capacitación sobre estos fenómenos cibernéticos es posible de brindarse a través de aplicaciones donde el usuario no requiere una concentración máxima que le provoquen aburrimiento o desinterés.

En [37] se desarrolló una ontología que abordó una solución semántica para la correcta gestión de la información, empleando una ontología FOAF (*Friend-of-a-Friend*, Amigo de un Amigo) estándar, la cual tiene la funcionalidad de definir el tipo de persona, las actividades y las relaciones de un individuo con otras personas, además es una ontología legible por máquina. La ontología desarrollada también hizo uso de ontologías de relaciones.

En [38] se desarrolló un sistema compuesto por una aplicación web y una móvil; La aplicación web funcionó como núcleo, pues es donde los datos fueron almacenados en un archivo RDF empleando vocabulario FOAF (*Friend Of A Friend*, Amigo de Un Amigo) y realizando las consultas con *SPARQL*. La aplicación móvil se empleó por los profesores, donde leyeron los datos de los estudiantes y permite que los docentes incorporen información sobre sus alumnos, por ejemplo la asistencia a clase, si el estudiante presento mala conducta o informar si su desempeño como estudiante decayó; esto con la finalidad de que se tomen medidas adecuadas para resolver este tipo de situaciones y ayudar a que mejore el desempeño académico del estudiante, además de mantener la opción de notificar a los padres del alumno sobre su desenvolvimiento en clase.

En el trabajo propuesto por [39] se desarrolló una aplicación móvil denominada CBMA (*Cyberbullying Mobile Application*, Aplicación Móvil de Ciberacoso) que tuvo como objetivo educar y brindar contenidos de cyberbullying a los adolescentes. Es una aplicación que se desarrolló en el sistema operativo iOS. Para su desarrollo se consideraron algunos criterios de *cyberbullying*, como lo son la difamación o menosprecio, revelar información personal de otra persona sin consentimiento de la misma o incluso hacerse pasar por otra persona, como la creación de cuentas falsas y en situaciones que están en relación con la sexualidad. Para el estudio del

cyberbullying percibido en los encuestados, se les aplicó una serie de cuestionarios a los mismos, antes y después del uso de la aplicación con el fin de conocer que tan informados se encontraban con el *cyberbullying*, para los cuales, se encuestaron a 125 estudiantes universitarios de pregrado y a 128 estudiantes de secundaria, dando como resultado que, en ambos grupos, no entendían lo que significa el *cyberbullying* y además no tenían el conocimiento de las herramientas para combatirlo. Los resultados después de darles el uso de la aplicación fueron satisfactorios en ambos grupos, sin embargo, el CBMA, dio un mejor desempeño en estudiantes de secundaria a comparación de los estudiantes de pregrado.

2.2. Análisis comparativo

En la Tabla 2.1 se presenta un análisis comparativo de los trabajos relacionados con el tema del presente proyecto de tesis; se incluye explicación breve del problema, la contribución propuesta, las tecnologías empleadas, el resultado obtenido y el enfoque.

Tabla 2.1 Análisis comparativo de artículos relacionados

Artículo	Problema	Contribución	Tecnologías	Resultado	Estado
Garaigordobil [20]	Determinar la relación existente entre la conducta antisocial y en la manera que implica situaciones de <i>bullying</i> y <i>cyberbullying</i> , así como las estrategias que emplean los jóvenes o adolescentes para la resolución de conflictos.	Identifica variables relevantes para el diseño de programas de intervención socioemocional para prevenir y/o reducir el comportamiento antisocial dirigido a los estudiantes.	Métodos de evaluación y recolección de información (autoinformes y cuestionarios).	Se obtuvieron perfiles psicológicos que presentaban los adolescentes, con respecto a las puntuaciones de conducta antisocial obtenidas, la posible relación en situaciones de <i>bullying/cyberbullying</i> y el estilo empleado para resolver conflictos.	Terminado
Ortega-Barón et al. [21]	Los jóvenes y adolescentes se encuentran en una postura más accesible hacia los medios digitales, lo que provoca el incremento de casos de <i>cyberbullying</i> y haciendo hincapié en que tipo de agresores hay.	Los análisis revelan que las variables de estudio predicen el ciberacoso, indicando que no existen efectos de interacción entre los niveles de implicación en ciberacoso y el género sobre la actitud hacia la autoridad y las conductas escolares violentas.	Método de recolección de información, específicamente 3 cuestionarios.	Se analizó la influencia de los niveles de participación en ciberacoso en tres grupos de adolescentes (no agresores, agresores ocasionales y agresores severos) sobre las variables psicosociales de actitud hacia la autoridad y la conducta escolar violenta.	Terminado.

Artículo	Problema	Contribución	Tecnologías	Resultado	Estado
Páez [22]	Determinar los factores que influyen en que una persona se torne ciberacosador.	Énfasis en que los ciberacosadores regularmente tienden a serlo por la poca relación positiva con sus padres, maestros o compañeros.	Métodos de recolección de información (encuestas) y la aplicación de regresión logística multivariada.	La agresión física, las asociaciones con compañeros que fuman cigarrillos o portan armas, la victimización previa por ciberacoso y la participación en el acoso tradicional están asociadas con la perpetración del ciberacoso.	Terminado.
Hang et al. [23]	Falta de investigaciones centradas en las instancias de ciberacoso.	Propuesta de un léxico de ciberacoso para las redes sociales.	<i>Enchanted Learning FrameNet</i>	El léxico de exclusión del ciberacoso originado, proporciona una referencia para los usuarios de las redes sociales y prevenir el ciberacoso.	Terminado.
Noviantho et al. [24]	Debido a la gran cantidad de información presente en internet, es difícil que los humanos rastreen todas las posibles instancias de ciberacoso.	Se determinó un modelo de clasificación con una precisión óptima para identificar conversaciones de ciberacosadores	Métodos de minería de texto, tales como <i>Naive Bayes</i> y <i>SVM (Support Vector Machine, Maquina de Vector Soporte)</i> .	El modelo más óptimo para clasificar las conversaciones de texto dirigidas a provocar una situación de ciberacoso, fue SVM con kernel poly; obteniendo 97.11% de precisión.	Terminado.

Artículo	Problema	Contribución	Tecnologías	Resultado	Estado
Upadhyay et al. [25]	Los casos de ciberacoso continúan incrementando y es común la práctica de <i>grooming</i> .	Sistema que clasifica las publicaciones y los comentarios de la red social Facebook, con la intención de detener situaciones de ciberacoso.	Algoritmo NLP (<i>Natural Language Processing</i> , Procesamiento del Lenguaje Natural). <i>Facebook</i> .	Con la implementación de este sistema es posible proteger a los niños, adolescentes y jóvenes de los ataques de ciberacoso, bloqueando el contenido malicioso de la plataforma digital.	Propuesta.
Farag et al. [26]	Regularmente se aplican técnicas de aprendizaje supervisado para la detección de casos de <i>cyberbullying</i> , sin embargo, se les da poca atención a otros enfoques, por ejemplo, los no supervisados.	Se determinaron algunos métodos eficaces de aprendizaje no supervisados para la detección de ciberacoso en diferentes plataformas digitales.	Técnicas de aprendizaje no supervisado, semi supervisado, codificadores automáticos, aprendizaje profundo y <i>clustering</i> (agrupamiento).	Examinación de las técnicas no supervisadas más efectivas para la detección del ciberacoso, ya que no se presta mucha atención a tales enfoques.	Propuesta.
Silva et al. [27]	Regularmente los adolescentes que sufren de <i>cyberbullying</i> , no recurren a sus padres o tutores para obtener ayuda; por lo tanto, el <i>cyberbullying</i> prevalece, incrementando las consecuencias del mismo.	Diseño e implementación de una aplicación móvil (<i>BullyBlocker</i>) que emplea un modelo holístico para la detección de ciberacoso en los adolescentes a través de la plataforma <i>Facebook</i> .	<i>Facebook</i> y herramientas para el desarrollo de aplicaciones móviles.	La aplicación <i>BullyBlocker</i> alerta a los padres sobre posibles casos de ciberacoso que presente su hijo, brindando información sobre qué hacer o a donde acudir para resolver este tipo de situaciones.	Terminado.

Artículo	Problema	Contribución	Tecnologías	Resultado	Estado
Akrim et al. [28]	Se cree que algunos adolescentes o jóvenes no son conscientes del fenómeno del <i>cyberbullying</i> , sus causas y consecuencias; ya que suele ser tomado como “broma” y no se le da la importancia requerida.	Da a conocer que los jóvenes si perciben el <i>cyberbullying</i> de distintas maneras y tienen posturas diversas ante el fenómeno.	Método de recolección de datos (encuesta).	Se encuentra que los estudiantes si tienen la misma percepción del ciberacoso en las redes sociales y la mayoría concuerda en los motivos de porque se originan los casos de <i>cyberbullying</i> .	Terminado.
Salawu et al. [29]	Los perpetradores de <i>cyberbullying</i> encuentran nuevas formas de llevar a cabo sus cometidos y aunque las plataformas digitales cuentan con sus propios filtros empleados para evitar este tipo de situaciones, muchos casos siguen ocurriendo.	Diseño e implementación de una aplicación móvil, denominada <i>BullStop</i> , la cual etiqueta los mensajes o comentarios recibidos por el usuario y de esta manera los clasifica de acuerdo a si es contenido ofensivo y lo elimina.	Modelos basados en aprendizaje profundo, uso de componentes <i>Synchroniser</i> o <i>Webhook</i> .	Por medio de la aplicación desarrollada es posible identificar instancias de ciberacoso e iniciar acciones automáticamente e, como eliminar mensajes ofensivos y bloquear a los acosadores en nombre del usuario.	Terminado.
Neo et al. [30]	Se cree que la mayoría de la sociedad ya cuenta con información solida sobre el <i>bullying</i> y el <i>cyberbullying</i> ; sin embargo, existen muchas carencias de estos fenómenos.	La aplicación <i>#StopBully</i> ofrece información acerca del <i>bullying</i> e intenta generar conciencia para mitigarlo, especialmente útil para captar la atención de niños o adolescentes.	Android Studio, Android SDK, JDK (Java <i>Development Kit</i> , Herramientas para el desarrollo con Java). <i>Adobe Photoshop</i> , <i>Paint 3D</i> y <i>Movie Maker</i> .	Se determinó que el uso de la aplicación si mejoro el conocimiento previo o nulo que tenían las personas sobre el <i>bullying</i> y el <i>cyberbullying</i> .	Terminado.

Artículo	Problema	Contribución	Tecnologías	Resultado	Estado
Chakraborty et al. [31]	Muchos de los mensajes ofensivos o con índole de ser mensajes de intimidación suelen estar emitidos por cuentas anónimas lo que resulta la difícil identificación de los tipos de mensajes inapropiados que ofenden al destinatario.	Ayuda a tener una comprensión mayor sobre las distintas formas en las que se utilizan las redes sociales (principalmente las de mensajería anónima) y los diferentes tipos de acoso presentes en los mensajes intercambiados.	Datos obtenidos de una API (<i>Application Programming Interface</i> , Interfaz de Programación de Aplicaciones) de <i>Twitter</i> basada en mensajes extraídos de la red social de mensajería anónima <i>Sarahah</i> .	Identificación de las diversas formas en las que se usa alguna aplicación donde los mensajes emitidos por los usuarios sean anónimos y si el hecho de que no se tenga un nombre como remitente de apertura a la presencia de acoso entre personas que ya se conocen. Además de categorizar el tipo de mensajes emitidos.	Terminado.
Kaiser et al. [32]	Los adolescentes o jóvenes que experimentaron alguna situación cercana con el ciberacoso, tienen un alto riesgo en desarrollar problemas de salud mental a corto o largo plazo.	Hacer énfasis en que, aunque es importante prevenir las situaciones de <i>bullying</i> o <i>cyberbullying</i> , también es importante darle un seguimiento correcto a las víctimas que pasaron por estas situaciones, pues se es sabido que existen casos con conclusiones graves.	Método de recolección de información y el uso de la aplicación móvil <i>NettOpp</i> .	Los resultados finales se pretenden obtener en el año 2023.	Propuesta.

Artículo	Problema	Contribución	Tecnologías	Resultado	Estado
Kutok et al. [33]	Se reporta que entre el 15% y el 70% de los adolescentes sufrieron de ciberacoso. Este fenómeno se asocia con una diversidad de consecuencias negativas, entre ellas el estado de ánimo depresivo.	Se emplearon diferentes redes sociales para hacer difusión sobre el tema del ciberacoso, proporcionando ayuda a los adolescentes que presencien un evento así.	Métodos de recolección de información (encuestas y entrevistas realizadas por <i>Google Meet</i>), uso de la aplicación <i>IMPACT</i> .	Se descubrió que los jóvenes estaban más satisfechos con <i>IMPACT</i> , el bienestar general y la intervención de los espectadores, así como con un menor estrés psicológico.	Terminado.
Foong y Oussalah [34]	Aunque existen plataformas diseñadas solo para compartir la libre opinión sobre algunas ideologías, estos medios llegan a ser utilizados para generar ciberacoso.	Proporciona un sistema automatizado cuya finalidad es detectar eventos de ciberacoso en foros y comunidades online.	Minería de datos (técnicas de clasificación), aprendizaje automático, ontologías difusas, SVM (<i>Support Vector Machines</i> , Máquinas de Soporte Vectorial) y el servicio <i>Amazon's Mechanical Turk</i> .	Capacidad de detectar situaciones de <i>ciberbullying</i> en comunidades online o foros públicos.	Terminado.
Thun et al. [35]	Muchos trabajos proponen técnicas para detectar el ciberacoso basándose en aprendizaje automático, pero sale en discusión el tema de la poca privacidad que tienen los adolescentes al momento de ser monitoreados con aplicaciones parentales.	Proporciona una aplicación móvil (<i>CyberAid</i>) capaz de detectar el ciberacoso, presentando una interfaz agradable y fácil de utilizar para los usuarios.	<i>Android Studio</i> , técnicas de minería de datos, conjunto de datos de entrenamiento obtenidos de <i>Twitter</i> y <i>Spyder</i> .	Se demostró que la aplicación móvil propuesta tiene una mayor precisión en la detección del ciberacoso que otras aplicaciones disponibles.	Terminado.

Artículo	Problema	Contribución	Tecnologías	Resultado	Estado
Singh et al. [36]	Falta de capacitación y comprensión sobre los temas relacionados con el ciberacoso, por parte de los niños.	Aplicación denominada MDEG, que capacita a los niños de educación primaria sobre el ciberacoso y como enfrentarlo.	Sin especificar.	Determina que para los niños el mejor medio de difusión sobre lo que es el ciberacoso, sus consecuencias y las opciones para enfrentarlo tienen que ser planteadas a través de herramientas didácticas, como por ejemplo un juego.	Terminado.
Olca y Can [37]	Los datos de los usuarios siempre cuentan con la máxima seguridad posible, pues existen personas o instituciones que buscan acceder a información privada sin el consentimiento de la o las personas involucradas.	Desarrollo de una ontología que permite gestionar el consentimiento de las personas con respecto al manejo de su información personal.	Uso de una ontología FOAF (<i>Friend Of A Friend</i> , Amigo de Un Amigo) estándar y diversas ontologías de relaciones.	Sin especificar.	Terminado.
Pérez Hernández et al. [38]	La tecnología no suele estar muy implicada en la educación presencial de las escuelas. Los profesores suelen llevar a cabo la gestión de sus alumnos y de las actividades realizadas de manera manual, en papel.	Diseño de aplicaciones (web y móvil) para la gestión de los datos de estudiantes y profesores, permitiendo también la gestión de las actividades desarrolladas en clase.	Android Studio con lenguaje de programación Java, <i>Framework JavaServer Faces</i> , <i>PrimeFaces</i> y vocabulario FOAF (<i>Friend Of A Friend</i> , Amigo de Un Amigo).	Detectar anomalías en la educación de un alumno con la finalidad de con las medidas adecuadas el estudiante mejore su desempeño.	Terminado.

Artículo	Problema	Contribución	Tecnologías	Resultado	Estado
Thinnukool et al. [39]	Los sitios web en Tailandia tienen problemas para brindar contenido informativo sobre el <i>cyberbullying</i> a las personas más jóvenes.	La aplicación CBMA (<i>Cyberbullying Mobile Application</i> , Aplicación Móvil de Ciberacoso) como una herramienta de ayuda para obtener información y ayuda para prevenir el <i>cyberbullying</i> en Tailandia.	Método de recolección de datos (encuesta). Sistema Operativo iOS.	Los adolescentes tailandeses no tienen conocimiento sobre el <i>cyberbullying</i> , la CBMA funciona como una herramienta de ayuda para los adolescentes para combatir y conocer el <i>cyberbullying</i> .	Terminado.

De todo el análisis anterior se concluye que, sin duda alguna el *bullying* y el *cyberbullying* son uno de los fenómenos que más acechan a los jóvenes y adolescentes, pues es más factible que se encuentren en una zona de vulnerabilidad y debido a esto se diseñan, desarrollan e implementan varias aplicaciones que tienen como objetivo detener y prevenir este tipo de acciones maliciosas. Existen muchas instituciones dedicadas a tratar de difundir información sobre como detectar la presencia de alguno de estos fenómenos, sin embargo, aún es muy común que ocurran; especialmente con el auge de las tecnologías de la información.

Se considera que la solución que se plantea en este proyecto es una herramienta que ayudará a prevenir pero también a actuar en dado caso que se identifique una situación de ciberacoso, pues México es un país con alto nivel de ciber acoso; los casos de acoso o ciberacoso ocurren tanto en instituciones públicas como en las privadas y aunque se desarrollaron otras aplicaciones que traten este tema, estas se diseñaron para utilizarse en un país ajeno, donde se habla un idioma diferente al español, los modelos que se emplean son basados en el lenguaje natural y existen ofensas dentro del ciberacoso que suelen ser más particulares de la zona donde se viva.

2.3. Propuesta de solución

En este capítulo se describe la propuesta de solución junto con la justificación de su selección para el anteproyecto presentado.

2.3.1. Descripción de la solución

Se propone desarrollar un módulo implementado sobre una aplicación móvil base que identifique situaciones de cyberbullying, empleando el procesamiento de lenguaje natural.

La aplicación base está diseñada empleando el patrón de diseño MVC (Model-View-Controller, Modelo-Vista-Controlador); por consiguiente, el presente proyecto continuara con esta arquitectura.

MVC es un patrón de diseño ampliamente utilizado para crear aplicaciones web y es usado en casi todos los marcos de desarrollo web. Como su nombre lo indica, este patrón está conformado por tres componentes, los modelos, las vistas y los controladores [40]. En los modelos se trabaja con los datos, con mecanismos para acceder a la información o para actualizar su estado. Las vistas contienen el código que permitirá la visualización de las interfaces con las que el usuario interactúa y los controladores contienen el código que permite responder a las acciones que se solicitan a la aplicación y que, de este modo, se vean reflejadas en las vistas. En la figura 3.1 se presenta de forma abstracta la arquitectura para este proyecto.

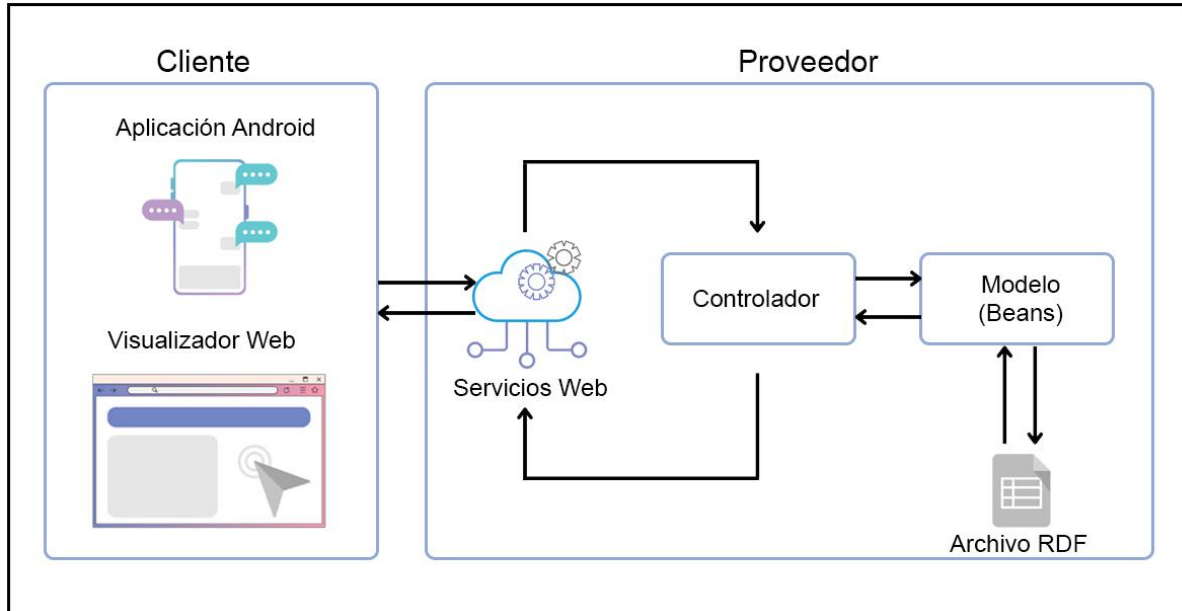


Figura 2.1 Patrón arquitectónico MVC aplicado en la aplicación propuesta.

La arquitectura de la aplicación se encuentra conformada en dos partes, el lado del cliente y el lado del proveedor, lo que permite una escalabilidad más factible para implementar el módulo a desarrollar. El cliente y el proveedor se comunican a través de servicios web basados en REST (*Representational State Transfer*, Transferencia de Estado Representacional).

Cliente. Es un demandante de servicios; se le conoce de esta forma al dispositivo que realiza peticiones y consume los servicios generados por el proveedor a través de la aplicación. El cliente dispone la vista de la aplicación que está conformada por interfaces compuestas por formularios, listas, imágenes, tablas, por mencionar algunos.

La aplicación móvil base se encuentra desarrollada para el sistema operativo Android por medio del Entorno de Desarrollo Integrado (IDE) Android Studio, que integra archivos XML (Extensible Markup Language – Lenguaje de Marcado Extensible);

además se plantea utilizar Java como lenguaje de programación para el consumo de servicios.

Proveedor. La aplicación base se encuentra gestionada por servicios web basados en REST. Existen diferentes alternativas de tecnologías para desarrollar este tipo de servicios, para el desarrollo del módulo se optará por el marco de servicios Jersey RESTful Web Service in Java por medio del lenguaje de programación Java.

Modelo. Representa la lógica de la aplicación en distintas clases encargadas de estructurar e interactuar con la información.

Controlador. Este componente se encarga de gestionar, atender y procesar las solicitudes recibidas del cliente. Con esto, el modelo y la vista se comunican para solicitar, procesar y pasar los datos necesarios a la vista para que pueda mostrarlos. Al ser un proveedor de servicios web basados en REST, tanto el proveedor como el cliente, devolverán y recibirán los datos en formato ligero para el intercambio de datos Notación de Objetos JavaScript (JSON).

2.3.2. Análisis de las tecnologías de información (TI)

En esta sección se presentan las Tecnologías de Información propuestas para abordar la problemática planteada. Algunas de las tecnologías empleadas continúan acorde a la aplicación base.

2.3.3. Lenguaje de programación

En este apartado se describe el lenguaje de programación que se utilizará para desarrollar el proyecto propuesto.

2.3.3.1. Java

Java se concibió por James Gosling, Patrick Naughton, Chris Warth, Ed Frank y Mike Sheridan en Sun Microsystems, Inc. en 1991 [41]. Es un lenguaje de programación y

una plataforma de desarrollo para una diversidad de aplicaciones (se utiliza para desarrollar aplicaciones móviles, aplicaciones web, aplicaciones de escritorio, juegos y mucho más). Por lo tanto, Java es empleado y ejecutado en diversos dispositivos, pues es un lenguaje multiplataforma rápido, seguro y fiable.

2.3.4. Marco de trabajo para el desarrollo de servicios REST

En este apartado se describe el marco de trabajo propuesto para el desarrollo de los servicios REST (GET, POST, PUT y DELETE) para el proveedor de la aplicación.

2.3.4.1. Jersey

El marco de trabajo de código abierto Jersey RESTful Web Services 2.x permite desarrollar servicios web RESTful en Java, brindando soporte para las API de JAX-RS. Asimismo, proporciona una API propia que amplía el rango de funciones y utilidades adicionales a las herramientas JAX-RS permitiendo la simplificación del servicio web RESTful utilizando Java [42].

2.3.5. IDEs

A continuación, se describen los IDEs (*Integrated Development Environment*, Entorno de Desarrollo Integrado) propuestos para llevar a cabo el desarrollo del proyecto.

2.3.5.1. NetBeans

Oracle donó el código fuente de Apache NetBeans a Apache Software Foundation en 2016. Con el paso del tiempo, muchos colaboradores se sumaron al proyecto. Apache NetBeans es un entorno de desarrollo integrado (IDE) de código abierto disponible gratuitamente para desarrollar aplicaciones web, de escritorio y móviles. Una de sus grandes ventajas es el soporte que proporciona para el ciclo de desarrollo, comprendiendo desde la creación del proyecto hasta la depuración, creación de perfiles e implementación. NetBeans proporciona editores, asistentes y plantillas para ayudar a crear aplicaciones en Java, PHP, C++, JavaFx y muchos otros lenguajes [43].

Asimismo, es ejecutable en varios sistemas operativos, tales como, Windows, Mac OS X, Linux, por mencionar algunos.

2.3.5.2. Android Studio

Anunciado en 2013 a través de una conferencia de Google I/O, Android Studio es un IDE (Entorno de Desarrollo Integrado, *Integrated Development Environment*) oficial para el desarrollo de aplicaciones del sistema operativo Android. Dicho entorno sirve para que las aplicaciones que se estén desarrollando sean mucho más eficientes; aunque el sistema operativo de Android se basa en el lenguaje de programación Java, Android Studio permite programar en otros lenguajes, como por ejemplo Kotlin, NDK y C++, empleando un sistema de compilación flexible basado en Gradle. Este IDE está basado en IntelliJ IDEA, que ofrece funcionalidades extra además de un potente editor de código y herramientas propias de IntelliJ para aumentar la productividad del desarrollo de aplicaciones [44].

2.3.6. Motor de base de datos

En esta sección se presenta el motor de base de datos que se propone para el desarrollo del presente proyecto.

2.3.6.1. Apache Jena Fuseki

Apache Jena Fuseki es un servidor SPARQL. Se ejecuta como un servicio de sistema operativo, como una aplicación web Java (archivo WAR), y como un servidor independiente [45]. Se encarga de exponer y recuperar las sentencias de un almacén RDF (Resource Description Framework, Marco de Descripción de Recursos) a través de HTTP y una API de estilo REST. El almacén RDF se define como una base de datos diseñada específicamente para almacenar y recuperar tripletas mediante consultas semánticas. Dichas tripletas son entidades de datos con la estructura sujeto-predicado-objeto.

2.3.7. Sistema operativo móvil

En esta sección se presenta el Sistema Operativo que se propone como alternativa para el desarrollo de este proyecto, puesto que la aplicación base se ejecuta sobre Android.

2.3.7.1. Android

Es el sistema operativo utilizado por 2.500 millones de dispositivos activos. Desde teléfonos 5G hasta las tabletas más sofisticadas [46]. Android incluye un sistema operativo basado en el kernel de Linux, una interfaz gráfica de usuario, un navegador web y aplicaciones descargables para el usuario final. Originalmente se desarrolló en 2003 por Android Inc. pero más tarde en 2005 se adquirió por Google, de esta manera la mayoría de los dispositivos con sistema operativo Android se encuentran preinstalados con un conjunto de software patentado, como Google Maps, YouTube, Google Chrome y Gmail. Cuando un usuario inicia un dispositivo, el sistema operativo Android muestra la pantalla de inicio, que es el centro de navegación principal para los dispositivos Android y se compone de widgets e íconos de aplicaciones.

2.3.8. Metodología

En esta sección se presenta la metodología propuesta para el desarrollo de este proyecto, enfatizando en que se empleará la misma metodología aplicada en la aplicación base de este proyecto.

2.3.8.1. Mobile-D

Es una metodología ágil, exclusivamente para el desarrollo de aplicaciones móviles, introducida en 2004 por Abrahamsson [47], desarrollada en cooperación con tres empresas enfocadas en el desarrollo de productos y servicios de software móvil. Se basa en metodologías de desarrollo bien conocidas, pero rigurosamente aplicadas en aplicaciones móviles, tales como: XP (eXtreme Programming, Programación Extrema) para las prácticas de desarrollo, Crystal Methodologies (Metodologías Crystal) empleado en la escalabilidad de métodos y RUP (Rational Unified Process, Proceso de Desarrollo Unificado) enfocado en la cobertura del ciclo de vida. La metodología

Mobile-D está optimizada para equipos de desarrollo de menos de 10 personas que trabajan en una oficina central, de modo que una aplicación móvil completamente funcional se entregue como producto final en poco tiempo (menos de 10 semanas según la metodología). La metodología Mobile-D involucra 5 iteraciones o fases: investigación, iniciación, producción, estabilización y prueba del sistema; cada uno asociado con tareas y prácticas.

2.3.9. Tecnologías para el procesamiento de lenguaje natural

Para implementar el procesamiento de lenguaje natural (NLP) se necesitan librerías o herramientas, las cuales se encuentran existentes para diversos lenguajes de programación; específicamente para el lenguaje de programación empleado en este proyecto (Java), se encuentran las siguientes.

2.3.9.1. Apache OpenNLP

Es una biblioteca Java de código abierto empleado para procesar texto en lenguaje natural, brinda un amplio abanico de servicios; OpenNLP es compatible con las tareas de PLN más comunes, como la tokenización, la segmentación de oraciones, el etiquetado de partes del discurso, la extracción de entidades nombradas, la fragmentación, el análisis, la detección de idiomas y la resolución de correferencias [48]. Estas herramientas se integran con otro software para ayudar en el procesamiento de texto, por lo que es una gran opción para los desarrolladores de software que están familiarizados con el desarrollo de software en Java. El sistema de compilación OpenNLP se basa en Maven.

2.3.9.2. Natural Language Toolkit

Natural Language Toolkit (NLTK) es una biblioteca de procesamiento de lenguaje natural (NLP) relevante en la construcción de programas en Python. Cuenta con un conjunto de bibliotecas para diversas tareas de procesamiento de texto, como clasificación, tokenización, derivación, etiquetado, análisis y razonamiento semántico e incluso permite realizar tareas más avanzadas como análisis semántico y construcción de modelos de lenguaje [49].

2.3.9.3. CoreNLP

CoreNLP desarrollado por Stanford NLP Group es un conjunto de herramientas de software de procesamiento de lenguaje natural que ayuda a las empresas a optimizar los procesos de extracción de datos, además de encontrarse disponible para 8 idiomas: árabe, chino, inglés, francés, alemán, húngaro, italiano y español. Ofrece módulos basados en Java para la solución de una gran cantidad de tareas básicas de PLN (permite derivar anotaciones lingüísticas para el texto, incluidos límites de tokens y oraciones, partes del discurso, entidades nombradas, valores numéricos y de tiempo, análisis de dependencia y circunscripción, correferencia, sentimiento, atribuciones de citas y relaciones [50]).

2.3.9.4. SparkNLP

La biblioteca de código abierto SparkNLP, se emplea para el procesamiento avanzado del lenguaje natural. SparkNLP se encuentra disponible para los lenguajes de programación Java, Python y Scala; además, cuenta con funciones tales como, tokenización, segmentación de palabras, normalizador, lematizador, coincidencia de expresiones regulares, coincidencia de texto, fragmentación, comparador de fechas, entre otros [51]. La biblioteca se basa en Apache Spark y su biblioteca Spark ML, la cual proporciona un conjunto de aplicaciones de aprendizaje automático que se compilan con dos componentes principales: estimadores y transformadores.

2.4. Alternativas de solución

De acuerdo con las características y necesidades del proyecto, se determinaron algunas alternativas de solución para abordar la resolución de la problemática anteriormente planteada. A continuación, se muestra la tabla 3.1 que contempla las posibles alternativas de solución al problema del proyecto.

Tabla 2.2 Comparación de alternativas de solución.

Alternativa	Metodología	Lenguaje de programación	Sistema operativo	Marco de trabajo para el servicio web	Motor de base de datos	IDE	Tecnología NLP
1	Mobile-D	Java	Android	Jersey	Apache Jena Fuseki	Android Studio, NetBeans	Apache OpenNLP
2	Mobile-D	Java	Android	Jersey	Apache Jena Fuseki	Android Studio, NetBeans	NLTK
3	Mobile-D	Java	Android	Jersey	Apache Jena Fuseki	Android Studio, NetBeans	CoreNLP
4	Mobile-D	Java	Android	Jersey	Apache Jena Fuseki	Android Studio, NetBeans	SparkNLP

Por la naturaleza del proyecto, debido a que se trata de un módulo sobre una aplicación base ya desarrollada, se determinó que se emplearán las mismas tecnologías para darle continuidad a lo ya establecido, por lo que, la diferencia se contemplara en la tecnología NLP (*Natural Language Processing*, Procesamiento de Lenguaje Natural) a utilizar.

En la alternativa número uno se contempla Java como lenguaje de programación, Android como sistema operativo móvil, Jersey como marco de trabajo para el servicio web, se emplea Apache Jena Fuseki como motor de base de datos, como entornos de trabajo se contemplan Android Studio y Netbeans; como metodología para el desarrollo del software se emplea Mobile-D y como tecnología para procesamiento de lenguaje natural, se contempla la biblioteca Java de código abierto Apache OpenNLP.

La segunda alternativa contempla las mismas tecnologías a excepción de la herramienta para trabajar el procesamiento de lenguaje natural, la cual es la biblioteca NLTK. De igual forma, la distinción de la tercera alternativa es la utilización del conjunto de herramientas de software de procesamiento de lenguaje natural proporcionado por CoreNLP.

Finalmente, la última alternativa contempla SparkNLP, que es una biblioteca de código abierto para el procesamiento avanzado del lenguaje natural.

2.5. Solución propuesta

Considerando las ventajas y desventajas de las tecnologías y herramientas analizadas, se determina como solución propuesta la alternativa número uno, detallada nuevamente en la Tabla 3.2.

Tabla 2.3 Solución Propuesta

Alternativa	Metodología	Lenguaje de programación	Sistema operativo	Marco de trabajo para el servicio web	Motor de base de datos	IDE	Tecnología NLP
1	Mobile-D	Java	Android	Jersey	Apache Jena Fuseki	Android Studio, NetBeans	NLTK

2.5.1. Justificación de la selección seleccionada.

La alternativa seleccionada para el desarrollo de la solución de este proyecto está ligada a la aplicación móvil base sobre la que se implementará el módulo. Siguiendo con la metodología Mobile-D ya que se centra exclusivamente en el desarrollo de aplicaciones móviles y se enfoca en la rapidez para desarrollar proyectos.

El lenguaje de programación es Java, debido a que es el lenguaje que maneja el IDE Android Studio, en el cual se desarrolló la aplicación móvil; además de continuar con la misma línea de desarrollo. Como motor de base de datos, se continua con Apache Jena Fuseki por la estructura sujeto-predicado-objeto debido a la semejanza a las estructuras del lenguaje natural. Para el lado del proveedor, se seleccionó el IDE Netbeans, porque provee un entorno favorable para la programación en el lenguaje Java. Como marco de trabajo para el servicio web, se encuentra Jersey pues es apto para Java.

Como tecnología NLP, se seleccionó NLTK, debido a la gran cantidad de documentación y herramientas que dispone, NLTK es modular y permite a los usuarios personalizar y combinar diferentes módulos según sus necesidades específicas. Esto proporciona una gran flexibilidad para adaptar las herramientas a los requisitos particulares de un proyecto. Además dicha biblioteca se encuentra dirigida a emplearse en Python, el cual es uno de los lenguajes de programación más populares para el desarrollo de aplicaciones de aprendizaje automático.

Capítulo 3. Aplicación de la metodología

El presente capítulo describe la metodología utilizada durante el desarrollo de la tesis de acuerdo con la problemática que se estudia en esta investigación, dividiéndose en dos secciones importantes. Como primera instancia, con la finalidad de comprender y analizar las limitantes de este proyecto, se aborda el apartado conceptual del fenómeno cyberbullying. Seguido de la contextualización de cyberbullying, este capítulo describe el proceso para el desarrollo del módulo de la aplicación móvil guiado por cada una de las fases de la metodología Mobile-D seleccionada en las alternativas de solución. Dicho módulo de la aplicación móvil permitirá al docente responsable del aula, identificar posibles situaciones de cyberbullying o mensajes negativos entre su grupo de estudiantes.

3.1. Cyberbullying: Origen, características, instrumentos y estrategias para la detección del fenómeno.

Patchin y Hinduja definen el ciberacoso como el uso de la tecnología de comunicaciones electrónicas como un medio para amenazar, dañar, avergonzar deliberadamente o aislar socialmente a otra persona [52], [53]. La comprensión del ciberacoso, las investigaciones y publicaciones resultantes de este fenómeno han crecido rápidamente durante la última década [54]. Sin embargo, a pesar de los esfuerzos realizados por la sociedad para mitigar este fenómeno, el cyberbullying se mantiene latente entre los jóvenes o adultos a través del internet y las redes sociales; pues de acuerdo con el módulo sobre ciberacoso 2021 del Instituto Nacional de Estadística y Geografía (INEGI) [55] el 22,8% de las mujeres y el 20,6% de los hombres que utilizaron Internet fueron víctimas de ciberacoso, cifras que indican una alta presencia del fenómeno.

En los trabajos de [56] y [52] se determina que las personas más propensas a ser víctimas o perpetradores de ciberacoso, son aquellas que tienden a usar por más tiempo Internet, alguna red social o su teléfono móvil y estadísticamente el grupo

comprendido por adolescentes son los principales miembros activos de las salas de chats o de populares redes sociales; por lo tanto, los jóvenes o adolescentes son los que regularmente se encuentran involucrados en casos de ciberbullying.

Aunque se tiene conscientemente la existencia del ciberbullying en todo el mundo, es difícil determinar la prevalencia exacta de este fenómeno, ya que para el ciberbullying es complicado determinar una frecuencia de repetición exacta con la que ocurren los eventos o cuanto tiempo dura un acto de ciberacoso (días, semanas o meses) [57]. De esta manera, el tiempo durante el que se prolongó el acto de ciberacoso sobre una persona y las circunstancias o características de la misma, influye en las consecuencias que se derivan a partir de ser víctima de este fenómeno, de acuerdo con los trabajos de [52], [54], [56], [58] y [59] las consecuencias pueden ser devastadoras para la víctima, incluyen resultados psicológicos y psicosociales negativos, son desde ira, tristeza, frustración, vergüenza, estrés, miedo, depresión, aislamiento, ansiedad, soledad y timidez hasta consecuencias más graves como el suicidio.

3.1.1. Origen del ciber acoso

Las agresiones y ofensas entre niños o adolescentes son un hecho que desde hace mucho tiempo se presentan en la sociedad, dichos comportamientos conjuntados con la repetitividad se denominan *bullying*. De acuerdo con la investigación de [54], [53] y [57] Olweus planteó por primera vez el termino bullying definiéndolo como “un comportamiento intencional para dañar a otro, repetidamente, donde es difícil para la víctima defenderse”.

Tradicionalmente el bullying incluye comportamientos distintivos como las agresiones físicas (p. ej., golpes o empujones) y agresiones verbales, tales como burlas o insultos, además de la exclusión y la difusión de rumores [60]. Con el incremento y avance tecnológico en las tecnologías de la comunicación, se han propiciado nuevas formas

de intimidación entre estudiantes o adolescentes, es aquí donde surge el nuevo termino asignado a este tipo de acoso que involucra el uso de dispositivos electrónicos.

Dentro de los pioneros en mencionar el término “cyberbullying” se encuentra Bill Belsey [61], quien primero se relacionó con el bullying tradicional, luego de esperar las noticias del tiroteo en la escuela secundaria Columbine en Middleton, Colorado y el tiroteo en la zona rural de Alberta, sucesos acontecidos con ocho días de diferencia en el año 1999; con las investigaciones realizadas se descubrió que los adolescentes que cometieron estos actos, sufrían de abusos por parte de sus compañeros, eran intimidados e insultados por un periodo de tiempo prolongado. Belsey decidió crear un sitio web “*www.bullying.org*” cuyos objetivos fueron ayudar a adolescentes que han sufrido acoso escolar, especificando que no es un suceso que deban de atravesar solos.

Poco después de la creación del sitio web, se dieron pie nuevos reportes en donde se manifestaban que los adolescentes sufrían de ofensas o intimidación a través de medios electrónicos que surgieron con el transcurso del tiempo, tales como el correo electrónico, los mensajes de texto en teléfonos móviles (SMS) y los mensajes multimedia (MMS), la mensajería instantánea, blogs y sitios web personales. En este punto, el educador canadiense Belsey, uso el termino cyberbullying, creado a partir del elemento compositivo cyber, (el cual indica la relación con redes informáticas y de comunicación) y del término bullying ya definido como acoso, definiéndolo así, como “el uso de las tecnologías de la información y la comunicación para apoyar el comportamiento deliberado, repetido y hostil de un individuo o grupo, con la intención de dañar a otros” [62], [63] y [64]; consecuente a este nuevo fenómeno, se creó el sitio web “*www.cyberbullying.ca*” cuyo objetivo fue centrarse en este tipo de acoso.

A partir del año 2000, se comenzaron las investigaciones sobre el fenómeno del cyberbullying en Estados Unidos, extendiéndose por otras partes del mundo, tales como Reino Unido y España [57]; dichas investigaciones continúan creciendo a la par de las nuevas plataformas digitales que se desarrollan y los medios a los cuales está

expuesto una persona. Aunque el estudio del ciberacoso es sólido y ya ha logrado mucho, enfrenta algunos desafíos importantes. En particular, los problemas de definición y medición deben abordarse de manera más completa [54].

3.1.2. Relación del cyberbullying con el bullying tradicional

Por mucho tiempo se ha debatido sobre la relación que existe entre el bullying tradicional y el ciberacoso, si alguno de los fenómenos desencadena a otro o si una persona que es víctima de esta situación sufre de los dos tipos de acoso al mismo tiempo. Si bien las investigaciones muestran que el acoso fuera de línea o "tradicional" tiene características similares y se correlaciona con las formas electrónicas de acoso, otros estudios muestran algunas diferencias significativas [58]. Dentro de las similitudes que algunos investigadores y educadores observan, son las consecuencias psicológicas que presentan las víctimas tras vivir alguna experiencia de algún tipo de agresión; dentro de las características de victimización se encuentra la autoestima baja, la depresión, la ansiedad o el estrés social. Muchos de estos efectos consecuentes a la intimidación suelen ser mayores en las personas que han experimentado ambos tipos de acoso. De acuerdo con la investigación de [58], no es sorprendente que la mayoría de las víctimas de ciberacoso también informen haber experimentado al menos una de las formas tradicionales de intimidación; esto sugiere que, si una persona se encuentra experimentando acoso cibernético, es probable que también experimente agresiones asociadas a bullying tradicional.

Muchas personas teorizan en que el acoso cibernético es solo una continuación del acoso tradicional a través de los nuevos medios (tales como las aplicaciones disponibles para los diferentes dispositivos móviles). Sin embargo, las personas que difieren con esta teoría, enfatizan en que el ciberacoso se diferencia del acoso tradicional en aspectos de gran relevancia, por ejemplo, el hecho de que un agresor cibernético puede mantenerse con facilidad en el anonimato, lo que complica la posibilidad de identificar al perpetrador o a la víctima. Por este motivo la mayoría de

los investigadores o personas interesadas en el tema, sugieren que ambos fenómenos comparten características comunes pero que tanto el acoso tradicional como el acoso cibernético son diferentes y que los perpetradores de cada fenómeno, tienen características particulares [65].

Algunos estudios, como [65] y [66], indican que las víctimas del acoso tradicional son más vulnerables o probables de sufrir ciberacoso, en algunas ocasiones un tipo de acoso desencadena otro, pues muchos estudiantes afirmaron que además de ser intimidados a través de dispositivos electrónicos, también fueron víctimas de agresiones en la escuela de manera presencial. Anteriormente impactaba la hipótesis de que el ciberacoso era más común o frecuente que el acoso tradicional, debido al gran auge que tienen las redes sociales y los medios de comunicación a través de los dispositivos electrónicos, sin embargo, existen comunidades o personas que no tienen gran accesibilidad a contar con estos medios de comunicación, especialmente en zonas rurales que es donde frecuente el bullying tradicional entre los niños y jóvenes.

Por otro lado, en las comunidades urbanas, es más común la accesibilidad a Internet, pues según el INEGI [67] la penetración de Internet casi se triplicó entre 2000 y 2015, la proporción de hogares con acceso a Internet aumentó del 18% en 2005 al 46% en 2015; por ende, es muy común que los adolescentes a corta edad cuenten al menos con un dispositivo móvil y dependiendo de las permisiones que proporcionan los padres, muchos de estos cuentan con alguna red social donde tienden a ser posibles víctimas de ciberacoso, es en este contexto que el ciberbullying suele ser más común que el acoso tradicional en las zonas urbanizadas. El ciberacoso es un problema social que sigue afectando a los adolescentes y, a medida que avanza la tecnología, existen cada vez más oportunidades para que este comportamiento dañino continúe [22].

3.1.3. Características del ciberbullying

El ciberbullying o ciberacoso es un término empleado para describir cuando una persona (sin importar edad, pero más comúnmente en niños y adolescentes) acosa,

amenaza, abusa o humilla a otra persona por medio de Internet u otros medios de comunicación, utilizando dispositivos electrónicos, tales como un teléfono móvil, una computadora o una tableta. El acoso cibernético incluye el acoso a través de medios electrónicos como mensajería instantánea, correo electrónico, salas de chat, sitios web, juegos en línea, sitios de redes sociales y SMS [65].

Las características principales del ciberacoso son la prevalencia de agresiones intencionales y comportamientos dañinos, ocurridos a través de un medio de comunicación y sobre todo acompañados de la repetitividad, cuyo objetivo es desequilibrar la balanza de poder entre los involucrados en el evento.

Dentro de otras características importantes del ciberacoso se encuentran las siguientes: el anonimato, ya que los ciberacosadores ocultan su identidad fácilmente a través de la red o del medio de comunicación empleado; la permanencia es una característica que indica la dificultad de que las publicaciones en línea se borren fácilmente, lo que afecta a largo plazo a la víctima.

Un claro ejemplo [67] es el primer caso de ciberacoso documentado y llamado “*Star Wars Kid*” protagonizado por un niño de 14 años que fue grabado en 2003 mientras simulaba una pelea de película, el video fue difundido por sus compañeros y rápidamente se expandió hasta el punto que hoy en día sigue disponible en algunas plataformas, el joven sufrió acoso y tuvo que cambiarse de escuela en repetidas ocasiones.

Otra característica del ciberacoso es la accesibilidad, ya que hoy en día el acceso a Internet y a las redes sociales es más común, haciendo que las personas se encuentren expuestas a sufrir este tipo de intimidación. De acuerdo con el INEGI [68] en su comunicado de prensa por el día mundial del internet (17 de mayo), en el año 2020 el 72% de la población mexicana hizo uso de internet y de las tecnologías de la información; además, el 60.6% de los hogares en México cuentan con acceso a internet, siendo el teléfono celular el dispositivo más empleado.

Como siguiente característica particular del ciberacoso, se encuentra la amplificación, la cual se refiere a la capacidad rápida de compartir información a través de internet, lo que puede aumentar el acoso sobre la persona a la que pertenezca la información difundida, tal como lo ocurrido con el caso anteriormente descrito “*Star Wars Kid*”. El ciberbullying contempla la característica de la virtualidad, lo que indica que, al ocurrir este fenómeno en línea, el acosador y la víctima pueden estar físicamente separados, permitiendo que estos eventos se lleven a cabo, aunque los involucrados no tengan una relación cara a cara o cercana.

3.1.4. Definición, ¿Qué vamos a entender por ciberbullying?

A medida que se desarrollan nuevas tecnologías y con ello nuevos medios de comunicación como las redes sociales, la interacción entre las personas se vuelve más rápida y eficiente. Desafortunadamente, estas herramientas permiten que el acoso tradicional o bullying cruce virtualmente los límites del espacio, llegando al ciberespacio, en donde se genera ciberacoso [69].

Este fenómeno virtual ha tomado diversas definiciones a lo largo de su prevalencia y como es mencionado en el trabajo de Chun [70] actualmente aún hay debates sobre la definición exacta o final del término de ciberbullying; muchos investigadores simplemente describen al fenómeno, como un tipo de acoso que ocurre a través del entorno en línea; pues a partir del concepto de bullying que propuso Olweus [64] donde lo define como “un ataque deliberado por parte de una o más personas, dirigido repetidamente contra una persona que no puede defenderse fácilmente”, se adoptó dicha definición para el acto de ciberbullying, como el bullying a través de un medio electrónico.

Por otro lado, algunos investigadores enfatizan en que hay diferencias entre el bullying tradicional y el ciberbullying [71], [72]; Smith definió al ciberbullying como un acto agresivo e intencional llevado a cabo por un grupo o individuo, utilizando formas electrónicas de contacto, repetidamente y a lo largo del tiempo contra una víctima que

no puede defenderse fácilmente [73]; la repetición de este comportamiento puede tener un efecto negativo en la salud mental y emocional de la persona afectada.

Otra definición de ciberbullying desarrollada a partir de la definición de bullying tradicional, es la propuesta por Hinduja y Patchin [74] que conceptualizan al fenómeno como “un daño intencional y repetido infligido mediante el uso de computadoras, teléfonos celulares y otros dispositivos electrónicos”. Aunque es relativamente fácil detectar el ciberacoso en forma de ataques repetidos directos, los incidentes tradicionales de acoso que antes se limitaban a un tiempo y lugar específicos ya no se limitan al ciberespacio, pues el contenido online es de fácil y rápida expansión.

De una manera más específica, Kowalski y Limber [60] mencionaron que el ciberacoso es “el acoso a través de correo electrónico y mensajería instantánea, en una sala de chat, en un sitio web o a través de un mensaje de texto enviado a un teléfono celular”, en esta conceptualización los investigadores mencionan los ciberespacios más comunes en donde ocurren este tipo de incidencias.

Por su parte, el gobierno de México define en su página oficial al ciberbullying como término utilizado para describir cuando un niño o adolescente es molestado, amenazado, acosado, humillado, avergonzado o abusado por otro niño o adolescente, a través de Internet o cualquier medio de comunicación como teléfonos móviles o *tablets*. De esta manera, el termino de ciberbullying se enfoca en menores, regularmente entre dos iguales; mientras que existen otros tipos de conductas que involucran a adultos, conocidas simplemente como ciberacoso o acoso cibernético, es decir que el gobierno de México establece esa diferenciación de términos [75].

Para efectos de este proyecto, se entenderá el ciberbullying como una conducta repetitiva de acoso entre pares, a través de correo electrónico, mensajes en línea, salas de chat, sitios web o mensajes de texto enviados a teléfonos móviles u otros dispositivos electrónicos. De este modo, el acoso involucra diferentes tipos de

agresiones, tales como insultos, apodos no consensuados, humillaciones, esparcir rumores o imágenes vergonzosas, etc.

3.1.5. Actores del ciberbullying

En el bullying y en el ciberbullying, ningún individuo está exento de sufrir alguno de estos hostigamientos o en peores casos, sufrir de ambos; en el mundo real, un acosador tradicional es posible que se convierta en víctima de acoso, por lo que un acosador cibernético también puede estar en línea y viceversa [56]. Muchos estudios e investigaciones [56], [76], [57] y [72] concuerdan que en el ciberbullying se involucran dos principales actores, los ciber agresores y las ciber víctimas, algunos involucrando los testigos o espectadores.

- **Ciber agresores:** es una persona que utiliza medios digitales, como las redes sociales, correo electrónico, mensajes de texto, entre otros, para acosar y hostigar a otros en línea. El ciberacosador o ciber agresor utiliza diferentes tácticas, como el acoso, la difamación, la intimidación y la exclusión social, para atacar a su víctima. De acuerdo con la investigación de Zych y Baldry [57], Cook, Williams, Guerra, Kim y Sadek descubrieron que los perpetradores exhiben un comportamiento de externalización, definido como un comportamiento agresivo, provocativo y perturbador descontrolado. Los perpetradores de ciberacoso se clasifican en dos [76], el actor principal y el actor auxiliar.
 - El perpetrador principal es la persona que desencadena o inicia la opresión de alguien que es víctima.
 - Los actores auxiliares son personas que participan en el envío de mensajes, participan en comentarios, participan en el envío de enlaces de imágenes o estados de videos, estas personas ya preceden al actor principal que contienen elementos de ciberacoso.
- **Ciber víctimas:** es una persona que ha sido objeto de acoso, hostigamiento, intimidación, difamación o cualquier otro tipo de agresión en línea. Esto incluye

mensajes de texto, correo electrónico, publicaciones en redes sociales, videos y fotos compartidas sin su consentimiento, y otras formas de ciberacoso. Las ciber víctimas regularmente experimentan un gran estrés emocional y psicológico, lo que tiene consecuencias graves en su vida diaria, como problemas de salud mental, ausentismo escolar o laboral, entre otros. De acuerdo con [72], [74] los jóvenes que participaron en más actividades en línea fueron más probabilidades de sufrir acoso en línea. Las víctimas de la intimidación a menudo tienen miedo de contarles a otros que están siendo intimidadas porque temen que la intimidación en realidad empeore si lo cuentan [61].

- Ciber espectadores: un espectador de cyberbullying es una persona que observa el acoso o la intimidación en línea que está siendo dirigido a otra persona. A diferencia de los participantes activos en el acoso, los espectadores no están involucrados directamente en la situación de acoso, pero aún tienen un papel importante que desempeñar para ayudar a prevenir y detener el acoso. Los espectadores optan por ser pasivos y no hacer nada al respecto, o pueden tomar medidas para apoyar a la persona afectada y detener el acoso.

3.1.6. Manifestaciones del cyberbullying

El ciberacoso conforme prevalece se crean nuevas maneras de acosar a las víctimas de este fenómeno, pues las tecnologías de la información avanzan y con ello la exposición a que una persona sufra de ciberacoso.

El cyberbullying puede manifestarse de varias maneras. De acuerdo con la investigación de Balakrishnan [5], Slonje [3] y [64] el ciberacoso incluye:

- Insultos, burlas, humillaciones o difamación en línea, pelea en línea que usa blasfemias y lenguajes hostiles, herir a alguien mediante la difusión de rumores maliciosos.
- Amenazas, tanto físicas como verbales.

- Acoso en redes sociales, como publicar mensajes ofensivos o inapropiados en los perfiles de las personas, enviar repetidamente mensajes ofensivos a alguien, acoso a través de mensajería instantánea (WhatsApp, Messenger, Facebook, SMS) [75].
- Publicación de imágenes o videos humillantes o comprometidos sin el consentimiento de la persona afectada, realizar publicaciones ofensivas en blogs, foros, sitios web y redes sociales (como Facebook, Twitter u otras) [75].
- Suplantación de identidad o robo de cuentas en línea, pretender ser otra persona y enviar mensajes para hacer que otra persona se vea mal.
- Aislamiento social, se manifiesta en la exclusión de grupos en línea o la difusión de rumores para alejar a la víctima de sus amigos y seres queridos.

Aunque existen distintos tipos de manifestación de ciberbullying, la más común es la agresión verbal a través de textos emitidos en mensajes o salas de chats, que se dirigen repetidamente a los estudiantes con una intensidad creciente. El acoso cibernético de esta forma suele tener lugar en las redes sociales a través de SMS, correo electrónico u otros servicios de comunicación. De acuerdo al estudio realizado por Kopecky [77], el 36.97% de la muestra de encuestados (139 de 376) sufrieron ciberacoso por medio de ataques verbales repetidos y prolongados; mientras que la segunda manifestación del ciberbullying más empleada por los ciberacosadores, es la amenaza, cuyo principal objetivo es implantar miedo en la víctima.

Por otra parte, Smith y colaboradores [73] establecen siete tipos de manifestaciones de ciberbullying: mensajes de texto recibidos en el teléfono móvil; fotografías o videos realizados con las cámaras de los teléfonos celulares, y posteriormente usados para amenazar a la víctima; llamadas acosadoras al teléfono celular; mensajes de correo electrónico insultantes o amenazantes; salas de chat en las que se arremete contra uno de los participantes o se le excluye socialmente; el acoso mediante los programas de mensajería instantánea; y páginas web donde se difama a la víctima, se descarga

información personal a la red o se hacen concursos en los que se ridiculiza a los demás.

Para efectos de este proyecto, se tomará la manifestación verbal a través de texto, con el objetivo de analizar dicho texto y de acuerdo a la repetitividad del acto, identificarlo como un posible caso de ciberbullying.

3.1.7. Manifestación verbal de violencia entre jóvenes

La comunicación entre los adolescentes suele ser diferente a la comunicación entre adultos, ya que, regularmente los adolescentes hacen uso de palabras catalogadas como “ofensivas” en la comunicación habitual con sus contemporáneos. Sin embargo, existen situaciones donde las palabras o mensajes emitidos conllevan otra intención, la cual es dañar a otra o a varias personas.

La violencia verbal es el acto de dañar a otra persona a través de mensajes o palabras; dichos mensajes suelen contener insultos, ironía o palabras tabú que causan efectos psicológicos sobre la víctima, por ejemplo, ansiedad, baja autoestima o depresión. Por lo tanto, la violencia verbal está íntimamente relacionada con la violencia social, ya que afecta directamente a la víctima e implica humillación ante la sociedad de tal manera que la capacidad social y autoconfianza se ven reducidas y afectadas [78].

Existen formas de agresión que son directas o indirectas en la forma en que se representan [64]. La violencia verbal se clasifica como un tipo de agresión directa, por lo que contempla una serie de características, las cuales son:

- Uso de palabras hirientes, insultos, amenazas o descalificaciones.
- Daño emocional a la víctima, como sentimientos de ansiedad, miedo, tristeza o vergüenza.
- Control o manipulación por parte del agresor, con el objetivo de ejercer poder sobre la víctima.

- Ocurren en cualquier relación o contexto, incluyendo el hogar, el trabajo, la escuela o en línea.
- Cualquier persona ejerce violencia verbal, independientemente de su edad o género.
- A menudo se normaliza la violencia verbal, se percibe como algo común (sobre todo entre los adolescentes) por lo que este tipo de agresión se minimiza y frecuentemente no se le da la debida importancia.

De acuerdo con [78] este tipo de violencia engloba comentarios degradantes, frecuentemente enfocados en el aspecto físico de la víctima, la inferioridad o la incompetencia, así como gritos, acusaciones, burlas o gestos de humillación. Los comentarios sarcásticos son frecuentes entre los jóvenes, pues prefieren la ironía para disfrazar el tipo de mensaje que pretenden dar hacia o sobre otra persona con objetivo de ridiculizarla o despreciarla. Uno de los ejemplos más comunes de violencia verbal son los apodos no consensuados, pues regularmente suelen estar dirigidos para resaltar un defecto físico o una acción. Esto demuestra que los adolescentes en la era digital actual son más agresivos e intimidatorios al ejercer violencia verbal en las redes sociales [76].

Con el uso de las TICs (Tecnologías de la información) se han incrementado los casos en los que una persona recibe mensajes maliciosos con contenido verbal ofensivo, es en este punto donde influye la duración o frecuencia con la que ocurren estas agresiones para tornarse en un evento de ciberacoso. Aunque el ciberacoso incluye diversos tipos de agresiones como, por ejemplo, la exclusión a un individuo de un grupo de chat, la publicación de una imagen vergonzosa o humillante, el lenguaje es el medio más importante al que los agresores de ciberbullying recurren a través de internet [79].

3.1.7.1. Tipo de manifestación de violencia verbal

La violencia verbal es un fenómeno que se extiende con el paso del tiempo, pues de acuerdo con las nuevas generaciones se generan nuevos tipos de insultos, bromas agresivas, temas controversiales por los cuales se generan comentarios hirientes y diferencias entre grupos. Cada sociedad, conscientemente o no, define lo que está bien y lo que está mal; qué palabras o gestos aceptar o rechazar; por lo tanto, la violación de estas normas conduce a la desestabilización de la armonía social, que sólo se restauran a través del diálogo [80].

Existen distintos tipos o incidencias de violencia verbal incluyendo:

- Acoso verbal: Repetir constantemente comentarios hirientes o humillantes hacia una persona.
- Intimidación: Amenazar o hacer sentir incómoda a alguien con palabras o acciones. Crear un entorno amenazante mediante la publicación de comentarios destinados a intimidar a otros o hacerles creer que se ven perjudicados al restringir la libertad de quienes son objeto de dicha violencia.
- Insultos: Decir palabras hirientes o despectivas hacia alguien con el propósito de herir sus sentimientos. Regularmente involucran el uso de peyorativos, es decir, palabras que descalifican, sobajan o menosprecian a la persona que las recibe. De acuerdo con el módulo de ciberacoso 2021 emitido por el INEGI [55] el 33.1% de la población de 12 años experimentó como situación de ciberacoso, la recepción de mensajes y llamadas ofensivas.
- Humillación pública: Hacer comentarios humillantes o ridiculizar a alguien en público.
- Chistes o bromas hirientes: Comentarios que parecen ser graciosos pero que en realidad tienen la intención de lastimar o humillar otra persona. Cualquier chiste o broma que hiere a alguien es violento, incluso si la persona que hace el chiste o la broma se defiende minimizando la situación.

De acuerdo con [76], en su investigación se determinaron los tipos de oraciones de ciberacoso más empleadas por los adolescentes; dichas oraciones con violencia verbal, se clasificaron en: oraciones que incluyen apodos, oraciones con amenazas a la seguridad física y oraciones con opiniones degradantes. Lo que rectifica que la violencia verbal entre los jóvenes se presenta de diferentes maneras, algunas de ellas se disfrazan de “simples burlas” o “juego” pero con la frecuencia en un tiempo prolongado tiende a transformarse en un tipo de acoso.

Sin duda el lenguaje verbal violento de los jóvenes cambia de acuerdo a las nuevas generaciones que van surgiendo, los insultos conocidos del año 2000 no son los mismos que los actuales, es por esto, que sería favorable el conocer los nuevos términos empleados por los jóvenes, para agredir a alguien más; sin embargo, en el contexto mexicano, no se contemplan estos diccionarios o bolsas de palabras que permitan identificar agresiones verbales por parte de los jóvenes.

Países como España, Venezuela o Chile, han abordado estudios que plantean las formas agresivas o violentas en las que se expresan los jóvenes de dichos países, tal es el caso de [80] o el diccionario de palabras “Hay palabras que matan” realizado en colaboración con varias instituciones de Chile, el cual contempla los términos más importantes relacionados con el ciberacoso y las palabras más frecuentemente utilizadas para agredir de manera verbal [81].

Debido a la falta de estudios e investigaciones sobre el lenguaje verbal violento entre los jóvenes mexicanos, se pretende realizar una investigación y consenso de primera mano, para obtener las palabras actuales con las que comúnmente se expresan los adolescentes o jóvenes en este ámbito; pues los insultos empleados en el lenguaje español mexicano, no son los mismos que se emplean en el español de otros países, como España, Chile, Colombia, entre otros.

3.1.8. Identificación del Cyberbullying a través de instrumentos y medios

Debido a que el ciberacoso es un fenómeno muy amplio, algunos investigadores tuvieron dificultades para saber cómo medir la prevalencia del mismo, en consecuencia, a esta incertidumbre, se han desarrollado instrumentos de medición sobre el cyberbullying; algunos de estos instrumentos son encuestas o cuestionarios para ser respondidos de manera personal o para que los padres y/o docentes respondan [57].

De este modo, diversos autores han creado sus propios instrumentos que, tras una serie de investigación y pruebas, se popularizaron de manera que son empleados en diferentes investigaciones o estudios del fenómeno del ciberacoso.

Los cuestionarios de autoinforme o mejor conocidos como encuestas, generalmente usan formatos de respuesta cerrados, como opciones dicotómicas y escalas de Likert (las cuales permiten que el encuestado, responda en qué nivel de acuerdo o desacuerdo se encuentran), lo que significa que los encuestados están limitados a las opciones de respuesta proporcionadas por el investigador, sin poder elaborar sus experiencias, opiniones o interpretaciones [82].

Las escalas de Likert, son las más empleadas en los instrumentos de medición de cyberbullying, por ejemplo, en el instrumento propuesto por [83]–[87] se emplean dichas escalas para que el encuestado responda su nivel de acuerdo o la frecuencia con la que le ocurren los hechos. Dichos instrumentos se encuentran compuestos por una cantidad de ítems [88] en donde las preguntas o afirmaciones contemplan el enviar un mensaje amenazante o intimidante a alguien, hacerse pasar por alguien, grabar un ataque a un teléfono celular, excluir a los compañeros en línea, por mencionar algunos ejemplos.

Dependiendo del instrumento de medición y del autor, estos se dividen en categorías, siendo las más comunes, la sección de ítems dirigidas a ser ciber víctima, ciber agresor o ciber espectador. Por ejemplo, en el estudio de [86] se emplea un instrumento de

medición que contempla las secciones de ciber victimización, en la que se plantean preguntas como “Alguien me ha dicho groserías o insultado por internet” y la sección de ciber agresión con preguntas como “He amenazado a alguien por internet o a través de mensajes de celular”.

Por otra parte, en [88] si se contemplan las tres secciones que involucran a los roles presentes en el ciberbullying, similares al cuestionario empleado en [86], las preguntas de ciber victimización se ejemplifican como “Recibí mensajes amenazantes o insultantes en el móvil (WhatsApp, Instagram, X...)”, en la sección de ciber agresión se toma como ejemplo la pregunta “Grabé un video o tomé fotos con el celular de algún compañero mientras realizaba algún tipo de comportamiento de naturaleza sexual”, para el apartado de ciber espectador se toman en cuenta preguntas como “Vi a alguien publicando chistes, rumores y chismes en Internet para avergonzar a un compañero de clase”.

Mientras que algunos instrumentos dividen los cuestionarios en secciones, otros autores solo se enfocan en un tipo de actor del ciberbullying, tal es el caso de [83] y [85] estudios que emplean un instrumento dirigido solo a los ciber agresores y en caso contrario, en [84] se enfoca en el rol de ciber víctima. El ejemplo de muchos instrumentos de medición de ciberbullying, demuestran que usar un diseño de investigación cualitativo y usar datos cualitativos para informar el desarrollo futuro de herramientas cuantitativas parece un enfoque más apropiado para capturar la fenomenología del ciberacoso [82] ya que, aunque se han desarrollado varios instrumentos para evaluar el ciberacoso desde 2004, existe una falta de conocimiento sobre sus propiedades psicométricas, de acuerdo con la revisión de [89], muchos instrumentos carecen de pruebas de validez y confiabilidad.

En la tabla 3.1 se exponen seis instrumentos de medición de ciberbullying empleados en diferentes trabajos de investigación, junto con sus principales características. Dichos instrumentos se han utilizado en diversos estudios para identificar el nivel del fenómeno de ciberbullying en pequeñas, medianas o grandes muestras; sin embargo,

en casos más específicos es complicado identificar la ocurrencia de los eventos de ciberacoso, además de que no es una detección rápida y al ser instrumentos donde la ciber víctima o el ciber agresor responden, se presta la situación de que no sean completamente honestos al responder, especialmente los ciber agresores, debido a que no se expondrían fácilmente por voluntad propia. Caso contrario, en las redes sociales o medios electrónicos, las personas se comportan con mayor libertad al no tener en cuenta que se encuentran bajo un instrumento de medición.

Tabla 3.1 Instrumentos de medición de cyberbullying

N°	Trabajos	Año	Dimensión	Ítems	Periodicidad	Edades	Subescalas	Fiabilidad	Validez
1	Alvarez-García, Barreiro-Collazo, Núñez, y Dobarro [83].	2016	Perpetración	19	Últimos tres meses Escala 1 al 4	12-18 años	3	rho de Raykov = .80	Validez discriminante
2	Buelga, Postigo, Martínez-Ferrer, Jesus Cava, y Ortega-Baron [84]. (CYBVICS)	2019	Victimización	18	Último año Escala 1 al 5	11-18 años	-	Alfa de Cronbach = 0.73	Validez convergente
3	Buelga, Postigo, Martínez-Ferrer, Jesus Cava, y Ortega-Baron [85]. CYB-AGS	2020	Perpetración	18	Último año Escala 1 al 5	11-18 años	-	.79-.90	Validez convergente
4	Brighi, A., Ortega, R., Pyzalski, J., Scheithauer, H., Smith, P. K., Tsormpatzoudis, H., Tsorbatzoudis, H [86]. ECIPQ	2012	Perpetración y victimización	22	0 = nunca 1 = una o dos veces 2 = una o dos veces al mes 3 = aproximadamente una vez a la semana 4 = más de una vez por semana.	10-19 años	2	No se menciona	No se menciona

5	Gonzalez-Cabrera, Leon-Mejia, Machimbarrena, Balea, y Calvete [87].	2019	Perpetración, victimización y ciberseguridad	35	0 = nunca 1 = algunas veces 2 = seguido	10-23 años	3	Coeficiente omega = .94	Validez convergente
6	Tiziana Pozzoli and Gianluca Gini - A self-report scale investigating [90].	2020	Perpetración, victimización, ciberdefensa, observador	16	Desde el comienzo del año escolar Escala 1 al 5	11-15 años	4	Alfa de Cronbach = 0.75	No se menciona

Al igual que existen los instrumentos de medición de ciberbullying para detectar la presencia de este fenómeno, también existen aplicaciones que permiten la prevención o detección del mismo. Dichas aplicaciones han surgido conforme los años y a las nuevas tecnologías, las cuales se enlistan a continuación.

- b-resol: Es una aplicación móvil cuyo objetivo es combatir el bullying, ciberbullying y los trastornos alimenticios presentes en los adolescentes. Permite alertar a los observadores o controladores parentales de alguna situación dañina para el adolescente [91].
- ReThink: Es una herramienta creada por Trisha Prabhu [92], la cual consiste en detectar mensajes ofensivos o hirientes y brindar a través del teclado móvil, recomendaciones para evitar el envío de estas palabras, por ejemplo, alertas o hacer una pausa para repensar o revisar las palabras empleadas con la finalidad de disminuir el odio al momento de usar chats.
- Proofup: Esta herramienta permite que los menores documenten el acoso en línea. Proofup no es una aplicación de control parental, los menores son los que eligen compartir contenido con sus padres o no. En adición, cuenta con un botón de alerta en caso de estar en peligro, el cual da aviso al tutor o tutores que se han puesto como protectora [93].

- Safetonet: La aplicación fue desarrollada en Reino Unido y alerta automáticamente a los niños y jóvenes cuando se detectan riesgos. También analiza el comportamiento en línea, identifica problemas, filtra riesgos y brinda recomendaciones en tiempo real en caso de identificar contenido dañino e ilegal [94].

Cabe señalar que, si bien existen aplicaciones que permitan la prevención o atención a casos de ciberacoso, muchas de estas no se encuentran dirigidas a la población mexicana, principalmente por el lenguaje verbal violento que se contempla en México; por lo que el desarrollo de este proyecto se presenta con una gran área de oportunidad.

3.1.9. Bolsa de palabras del lenguaje verbal violento entre jóvenes

Ya que el objetivo de este proyecto es la detección de ciberbullying a través de lenguaje natural, será analizada la parte textual de los medios digitales y es necesario obtener la bolsa de palabras empleadas por los jóvenes para agredir, humillar, desacreditar u ofender a alguien más. Sin embargo, como se mencionó con anterioridad, en México no se contemplan diccionarios o bolsas de palabras que permitan identificar las agresiones verbales a través de medios digitales por parte de los jóvenes o adolescentes. Para lo cual, como primer punto se clasificaron las dimensiones a abordar en relación con las manifestaciones del ciberbullying; de esta manera, se contempló la dimensión de burla, amenaza e insulto.

La tabla 3.2 expone cada una de las dimensiones a abordar y para que dichas dimensiones se puedan operacionalizar se estableció su significado dirigido a este proyecto, así como los medios a través de los cuales se manifiesta y los resultados o consecuencias del acto.

Tabla 3.2 Dimensiones de las manifestaciones de ciberbullying.

Dimensión	Significado	Medio	Resultado
Burla	Es el acto o conducta de provocar la vergüenza de una persona por diversión para ridiculizarlo; puede ser divertido u ofensivo según la ambigüedad de la situación, debiéndose a las interacciones personales de los humanos.	▪ Chistes ▪ Bromas ▪ Ironía	▪ Herir ▪ Humillar ▪ Ridiculizar ▪ Desacreditar ▪ Discriminar
Amenaza	Se refiere a la acción de expresar o hacer algo que sugiere la posibilidad de causar daño o peligro a alguien o algo. El objetivo de la amenaza es infundir miedo o intimidación en la otra persona para lograr algún resultado deseado.	▪ Frases que infunden miedo ▪ Ataque a la vulnerabilidad de la persona	▪ Intimidar ▪ Controlar

Insulto	Los insultos son utilizados de manera intencional para causar daño emocional a otra persona. Puede ser una palabra, frase, comentario o gesto que se utiliza para atacar a alguien de manera ofensiva e hiriente.	▪ Apodos ▪ Palabras antisonantes ▪ Palabras despectivas	▪ Ofender ▪ Menospreciar ▪ Herir ▪ Humillar ▪ Discriminar ▪ Excluir
----------------	---	---	--

Ya delimitadas las dimensiones a abordar, se formularon una serie de preguntas enfocadas a cada una de las dimensiones, teniendo un total de 11 ítems (Tabla 3.3).

Objetivo del cuestionario: Recolectar palabras y frases con la finalidad de insultar, burlarse o amenazar a través de las redes sociales por parte de jóvenes universitarios.

Tabla 3.3 Ítems clasificados por dimensión.

Dimensión	Ítems
Burla	En las redes sociales, por medio de los chats, en comentarios, publicaciones... ▪ ¿Qué frases o palabras has identificado, con el propósito de discriminar a una persona? ▪ ¿Qué chistes has identificado cuyo objetivo sea ridiculizar a una persona? ▪ Si has observado alguna ironía que tenga por objetivo humillar a una persona, descríbela.
Amenaza	En las redes sociales, por medio de los chats, en comentarios, publicaciones... ▪ ¿Con que frases o palabras has identificado que una persona amenaza a otra? ▪ ¿Qué frase considerarías una amenaza? ▪ ¿Qué frase considerarías una amenaza con la finalidad de controlar a otra persona?
Insulto	En las redes sociales, por medio de los chats, en comentarios, publicaciones... ▪ ¿Cuál es el insulto más común que hayas visto? ▪ ¿Cuál es el insulto más ofensivo que hayas visto? ▪ ¿Qué groserías has identificado? ▪ ¿Qué insultos, a través de abreviaturas has visto? Y ¿Cuál es su significado? ▪ ¿Qué apodos ofensivos has visto?

Posteriormente se añadieron las preguntas a un cuestionario en Google Forms (figura 3.1) con la finalidad de que su distribución fuera más accesible y se distribuyó el enlace con jóvenes universitarios de la licenciatura en Administración de la Universidad Autónoma del Estado de México y de estudiantes de las ingenierías de Sistemas Computacionales, Gestión Empresarial y Química del Instituto Tecnológico de Orizaba.

Enlace al cuestionario: <https://forms.gle/t8sXH1pHbP4wHkDX9>



The image shows a Google Forms interface. At the top, there is a dark blue header with the word "CYBERBULLYING" in large, bold, white capital letters. Below the header is a row of icons representing various aspects of cyberbullying: a person with a speech bubble, a person with a speech bubble and a "HATE" label, a person with a speech bubble and a "HATE" label, a person with a speech bubble and a "HATE" label, a person with a speech bubble and a "HATE" label, a person with a speech bubble and a "HATE" label, a person with a speech bubble and a "HATE" label, a person with a speech bubble and a "HATE" label, a person with a speech bubble and a "HATE" label, and a person with a speech bubble and a "HATE" label.

Below the header, the main title of the form is "Violencia verbal entre jóvenes" in bold black text. Underneath the title, there is a paragraph in Spanish that reads: "Objetivo: El objetivo del presente cuestionario, es identificar frases o palabras ofensivas dentro del entorno virtual-digital como parte del fenómeno del ciberbullying." Below this, another paragraph states: "Los resultados serán utilizados únicamente con fines académicos y de investigación. Su contribución apoyará al desarrollo de estrategias para disminuir este fenómeno entre jóvenes, por lo que su participación es muy importante. Cabe mencionar, que los datos obtenidos serán utilizados de forma anónima."

Figura 3.1 Formulario creado en Google Forms.

La recopilación de la información fue autoadministrada y se llevó a cabo en un periodo de aproximadamente dos semanas; gracias a la herramienta de Google Forms, las respuestas se almacenaron en hojas de cálculo de Excel (figura 3.2).

Figura 3.2 Previsualización de las respuestas obtenidas.

Las respuestas obtenidas fueron tratadas a través del software Atlas.ti [95] realizando un análisis cualitativo para determinar la repetitividad de las palabras y contemplar las palabras más comunes en el lenguaje verbal violento empleado en el grupo poblacional comprendido por jóvenes universitarios. De igual forma se analizó la repetitividad de las palabras en cada una de las dimensiones comprendidas y posteriormente se realizó la depuración de aquellas palabras que no se relacionaban directamente con el propósito inicial como, por ejemplo, conectores y artículos (figura 3.3).

	A	B	C	D	E	F	G	H	I	J	K
1	Total	Palabra	Largo	1. Dimensión burla	%	2. Dimensión amenaza	%	3. Dimensión insulto	%	Total	%
2	179	pendejo	7	8	0.21%	3	0.07%	168	4.16%	179	1.96%
3	130	puta	4	0	0.00%	3	0.07%	127	3.15%	130	1.42%
4	127	madre	5	0	0.00%	19	0.47%	108	2.68%	127	1.39%
5	110	negro	5	64	1.66%	1	0.03%	45	1.11%	110	1.20%
6	99	verga	5	1	0.03%	5	0.12%	93	2.30%	99	1.08%
7	82	hijo	4	2	0.05%	2	0.05%	78	1.93%	82	0.90%
8	80	puto	4	10	0.26%	0	0.00%	70	1.73%	80	0.88%
9	65	gordo	5	29	0.75%	0	0.00%	36	0.89%	65	0.71%
10	61	idiota	6	6	0.16%	1	0.03%	54	1.34%	61	0.67%
11	54	persona	7	30	0.78%	11	0.27%	13	0.32%	54	0.59%
12	53	chinga	6	0	0.00%	1	0.03%	52	1.29%	53	0.58%
13	51	color	5	45	1.17%	0	0.00%	6	0.15%	51	0.56%
14	45	ctm	3	0	0.00%	0	0.00%	45	1.11%	45	0.49%
15	36	fisico	6	19	0.49%	1	0.03%	16	0.40%	36	0.39%
16	36	mierda	6	1	0.03%	1	0.03%	34	0.84%	36	0.39%
17	35	más	3	8	0.21%	14	0.34%	13	0.32%	35	0.38%
18	35	ninguno	7	8	0.21%	0	0.00%	27	0.67%	35	0.38%
19	33	gorda	5	15	0.39%	0	0.00%	18	0.45%	33	0.36%
20	33	vete	4	1	0.03%	2	0.05%	30	0.74%	33	0.36%
21	32	personas	8	24	0.62%	2	0.05%	6	0.15%	32	0.35%
22	27	piel	4	24	0.62%	0	0.00%	3	0.07%	27	0.30%
23	27	ptm	3	0	0.00%	2	0.05%	25	0.62%	27	0.30%
24	26	tienes	6	13	0.34%	11	0.27%	2	0.05%	26	0.28%
25	25	digo	4	0	0.00%	25	0.62%	0	0.00%	25	0.27%
26	25	zorrra	5	0	0.00%	0	0.00%	25	0.62%	25	0.27%
27	24	hdp	3	0	0.00%	0	0.00%	24	0.60%	24	0.26%
28	23	prieto	6	13	0.34%	0	0.00%	10	0.25%	23	0.25%

Figura 3.3 Previsualización de la lista de palabras.

Dentro de la lista de palabras se destacan cinco términos más empleados en todas las dimensiones, se muestra una representación en la gráfica siguiente (figura 3.4).

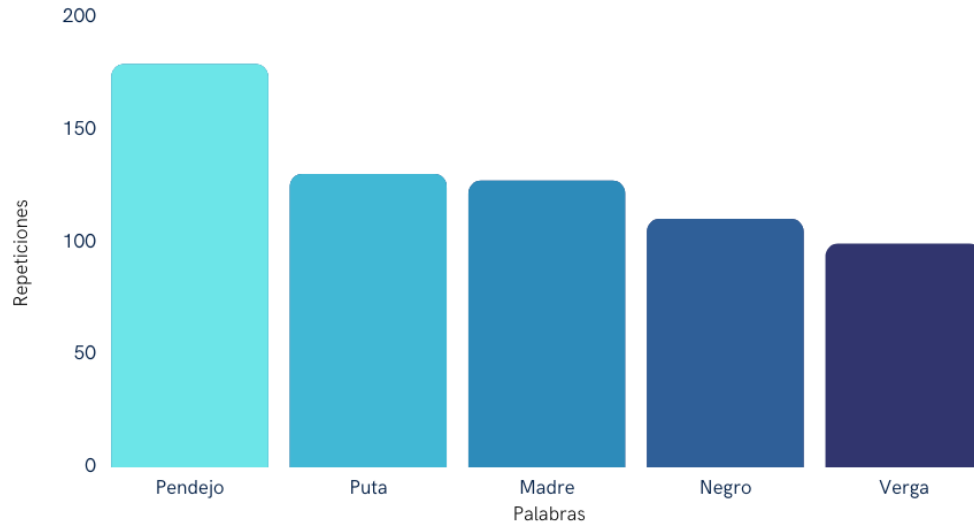


Figura 3.4 Representación gráfica de términos más empleados

Así como la lista de palabras, Atlas.ti también proporciona las nubes que representan la repetitividad de las palabras de forma gráfica (figuras 3.5, 3.6, 3.7, 3.8).

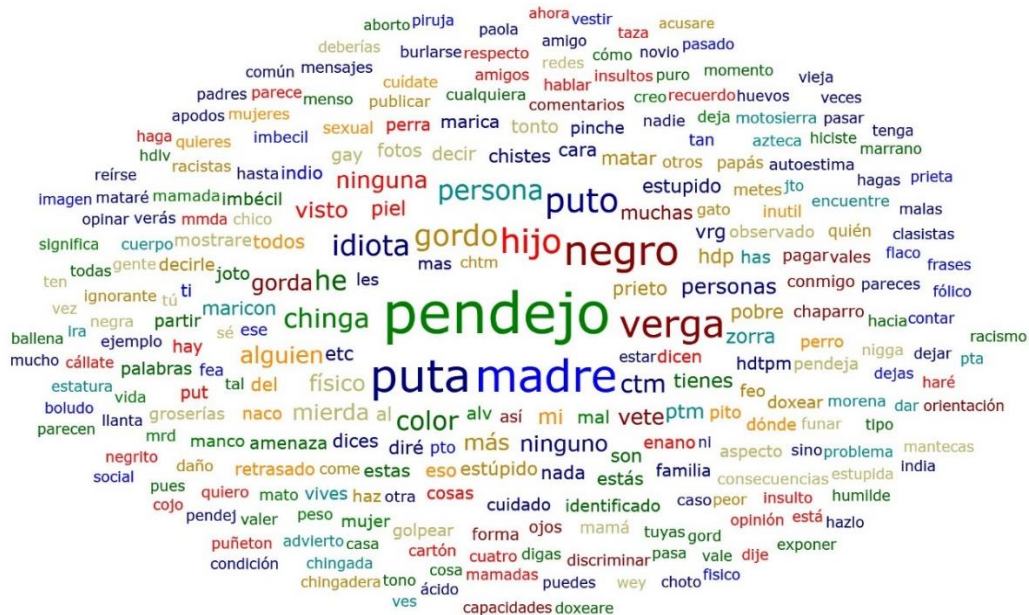


Figura 3.5 Nube que contempla todas las dimensiones.

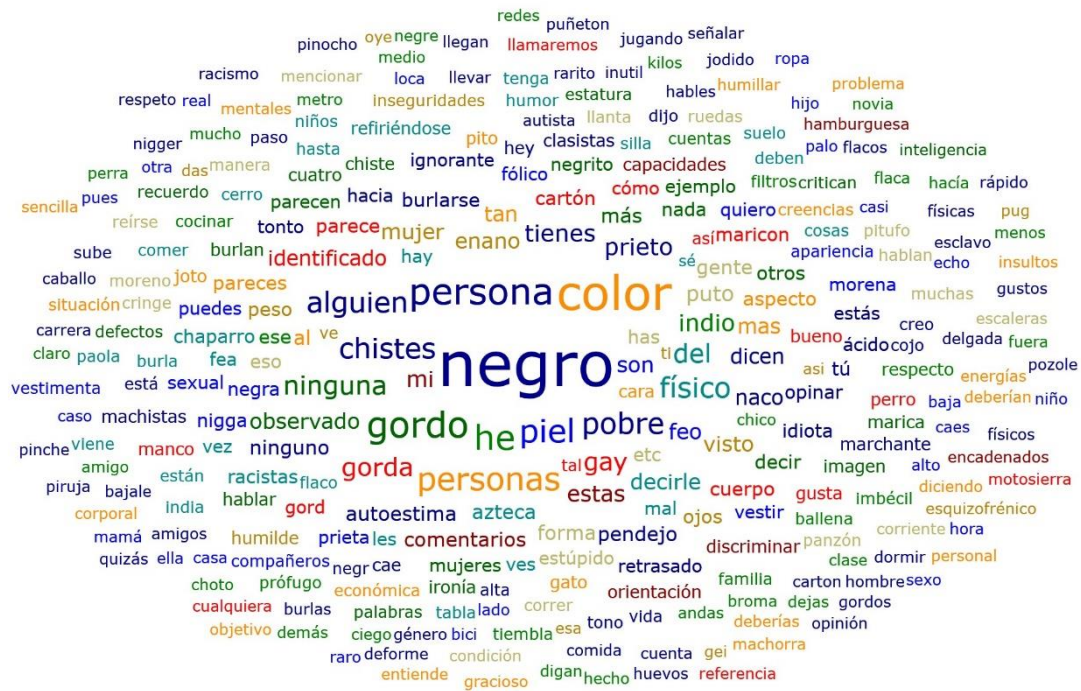


Figura 3.6 Nube de la dimensión "Burla".



Figura 3.7 Nube de la dimensión "Amenaza".

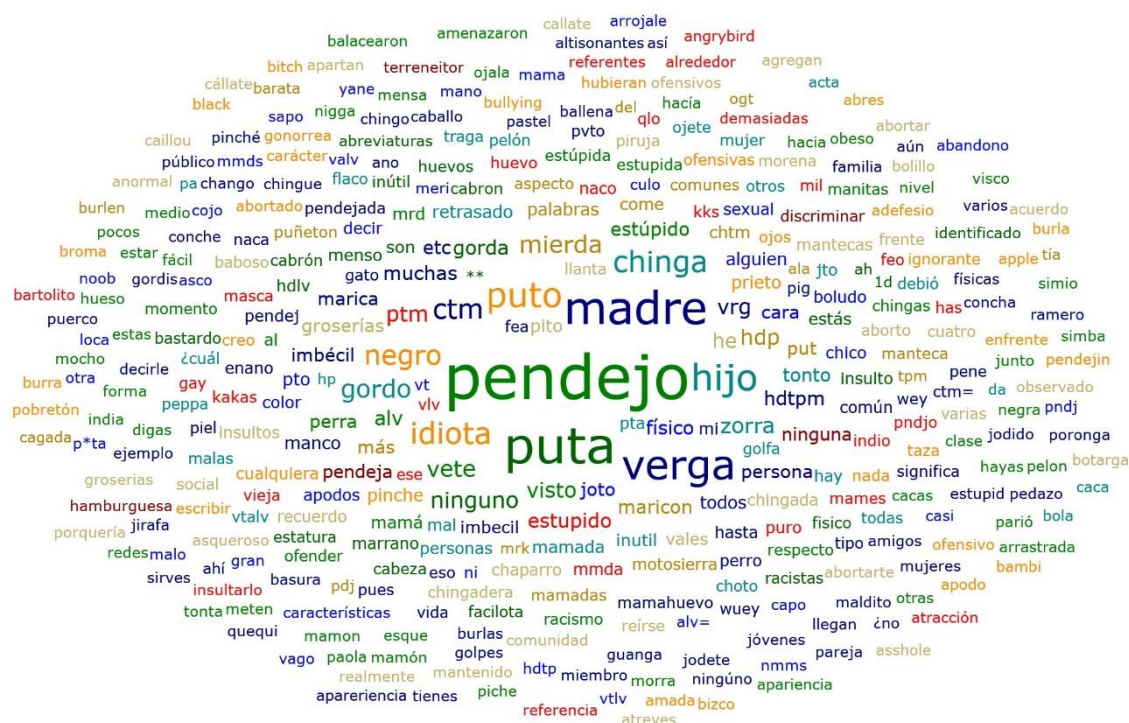


Figura 3.8 Nube de la dimensión "Insulto".

3.2. Aplicación de la metodología Mobile-D en el desarrollo del módulo de la aplicación móvil

Al igual que en la aplicación móvil base de este proyecto, se hará uso de la metodología Mobile-D en el desarrollo del presente módulo. La metodología Mobile-D comprende 5 fases o etapas: exploración, iniciación, producción, estabilización y pruebas del sistema. En la etapa de exploración, se definen los roles y responsabilidades de los actores involucrados en el proyecto. En la fase de iniciación se preparan e identifican todos los requisitos necesarios. Se elaboran los planes para las próximas fases y se establece el entorno técnico; en las fases de producción y estabilización se llevan a cabo aquellas actividades de desarrollo, programación o codificación de la aplicación, realizando dichas actividades repetidamente hasta implementar todas las funcionalidades, por último en la fase de pruebas del sistema

se contempla la finalización de la aplicación en su versión estable y se realizan las pruebas pertinentes para asegurar el correcto funcionamiento del sistema. La figura 3.9 muestra gráficamente el proceso de la metodología Mobile-D.

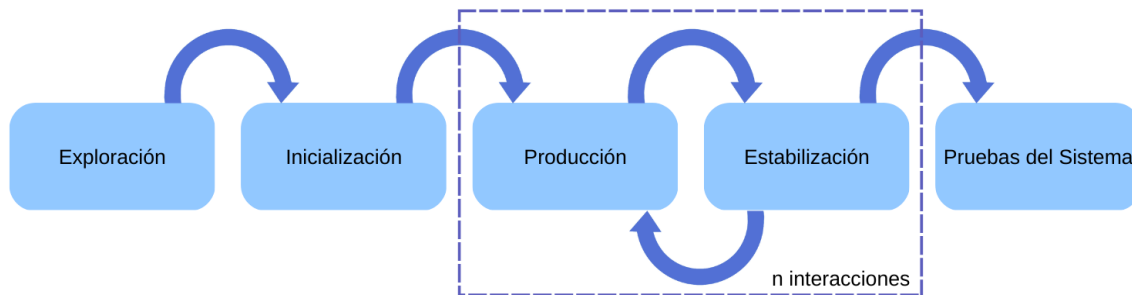


Figura 3.9 Proceso correspondiente a la metodología Mobile-D.

3.2.1. Exploración

Esta fase implica definir los objetivos del proyecto, establecer los requisitos iniciales a partir de la delimitación conceptual anteriormente descrita y describir las especificaciones del producto, así como establecer un plan de acción para el desarrollo.

3.2.1.1. Establecimiento de los interesados

A continuación, se describen las personas o actores involucrados en el desarrollo del módulo de la aplicación.

- Desarrollador

Al ser ingeniera en sistemas computacionales, se encarga de analizar requerimientos y especificaciones del sistema, desarrollar el módulo de la aplicación, implementar el módulo en la aplicación móvil base, realizar las pruebas pertinentes y documentar el producto de software.

- Director

Se encarga de supervisar y dirigir el proyecto de tesis, participando en la toma de decisiones con el objetivo de orientar, retroalimentar y apoyar al alumno en las diferentes etapas del proceso de investigación y desarrollo del producto de software.

- Jurado

Es un comité de maestros, doctores, investigadores y expertos que evalúa el trabajo desarrollado, brindando observaciones o sugerencias que permitan cumplir con los estándares de calidad esperados en el proyecto.

- Grupo DIPAAM (Acompañamiento y valoración)

Ubicado en Apizaco, Tlaxcala; es una institución que ofrece servicios de atención profesional en materia de salud mental, brindando tratamientos y atendiendo padecimientos de atención psicológica y mental. Grupo DIPAAM se encarga de dar seguimiento al trabajo realizado en este proyecto, atendiendo el apartado del fenómeno ciberbullying.

3.2.1.2. Definición del alcance

En esta sección se describe la planeación inicial del proyecto, contemplando las dependencias, supuestos y limitaciones; además, se plantean los requisitos iniciales del proyecto.

- Dependencias

Las dependencias en el desarrollo del módulo de la aplicación se describen a continuación:

- Se obtendrán los tweets de los alumnos por medio de la API de X (antes conocida como Twitter) v2.
- El algoritmo para identificar situaciones de alerta con respecto a posibles casos de ciberacoso, partirá de la bolsa de palabras.
- El grupo de alumnos, será correspondiente a los alumnos registrados a través de la aplicación base.

- **Supuestos**

Los supuestos en el desarrollo del módulo son los siguientes:

- El módulo se encuentra orientado a ser utilizado en el contexto estudiantil, partiendo de un salón de clases donde se obtenga acceso a los tweets de los alumnos involucrados.

- **Limitaciones**

A continuación, se describen las limitaciones para el desarrollo del módulo de la aplicación móvil.

- La aplicación móvil base se encuentra destinada a ser empleada en dispositivos móviles con sistema operativo Android (versión 8.0 o superior), por lo que el módulo tendrá las mismas limitaciones.
- Se requiere de conexión a internet para el almacenamiento de la información y para la obtención de los datos emitidos por la API de X.
- Ya que la aplicación se encuentra diseñada para funcionar con un determinado grupo de alumnos, es necesario que la población de estudiantes quede registrada y delimitada, para posteriormente agregar su perfil de la red social X.
- Ya que el módulo contempla la detección de ciberacoso a través de la red social X, los participantes involucrados tendrán que tener un perfil en dicha red social.

3.2.1.3. Requisitos iniciales

En el presente proyecto se desarrollará un módulo para una aplicación móvil base Android, que tenga por objetivo la detección de posibles casos de ciberacoso en la red social X empleando procesamiento de lenguaje natural. Contemplando el análisis previamente descrito, se determinaron los siguientes requisitos funcionales (tabla 3.4) y requisitos no funcionales (tabla 3.5).

3.2.1.3.1. Requisitos funcionales

Tabla 3.4 Requisitos funcionales

ID	Requisito	Descripción	Prioridad
RF1	Autenticación de usuario	El docente iniciará sesión en la aplicación para poder acceder al módulo, mediante sus credenciales (correo electrónico y contraseña).	Alta
RF2	Consultar grupo	El docente podrá observar el listado de su grupo.	Alta
RF3	Agregar usuario X	El docente podrá seleccionar un alumno del listado de su grupo y registrar el username de X correspondiente del alumno.	Alta
RF4	Consultar tweets de alumno	El docente podrá acceder a un apartado para consultar los tweets emitidos de cada alumno.	Alta
RF5	Consultar Likes y Retweets	Así como los tweets emitidos, el docente también podrá observar un listado de los usuarios que han dado like o retweet.	Media
RF6	Consultar últimos tweets de alumnos	En un apartado del módulo se podrán observar los últimos tweets realizados por todo el grupo, limitando la lista a 20 tweets.	Alta
RF7	Consultar situaciones de alerta	En el apartado de situaciones de alerta, el docente podrá observar aquellos tweets con contenido sensible que se hayan detectado a través del algoritmo para identificar posibles situaciones de ciberacoso,	Alta

		haciendo énfasis en el texto del tweet y el usuario que lo emitió (Últimos 3 días).	
RF9	Generar reporte	El docente podrá seleccionar la opción para que la aplicación genere un reporte con la información recolectada.	Media

3.2.1.3.2. Requisitos no funcionales

Tabla 3.5 Requisitos no funcionales

ID	Requisito	Descripción	Prioridad
RNF1	API Twitter	Es necesaria la disponibilidad de la API de Twitter para poder obtener los tweets e información necesaria de la plataforma.	Alta
RNF2	Plataformas	Ya que la aplicación móvil base se encuentra destinada a usarse en dispositivos Android, el módulo también será ejecutado en dicho sistema operativo.	Alta
RNF3	Almacenamiento	La aplicación base y el módulo utilizan almacenamiento de tripletas proporcionado por Apache Jena Fuseki por medio del vocabulario FOAF.	Alta
RNF4	Idioma	Al no contar con ajustes de internacionalización, el idioma por defecto de la aplicación es el español, de igual forma la identificación de ciberacoso se encuentra dirigida al contexto mexicano.	Media
RNF5	Población	La aplicación está contemplada a ser utilizada en un único salón de clases con un docente durante una jornada de estudios o un ciclo escolar determinado.	Alta

3.2.2. Inicialización

En esta fase se prepara el plan de desarrollo del proyecto y se establece el entorno técnico.

3.2.2.1. Puesta en marcha del proyecto

Se indican las características necesarias para la elaboración de la aplicación, indicando los recursos técnicos y humanos necesarios para el desarrollo de la misma.

- Tipo de proyecto: Módulo de una aplicación nativa.
- Entorno de desarrollo para la aplicación móvil (cliente): Android Studio
- Entorno de desarrollo para el proveedor de servicios: NetBeans
- Editor de código fuente para proveedor de servicios: Visual Studio Code
- Aplicación para desarrollador: Twitter Developer
- Servicio externo: API Twitter v2

3.2.2.1.1. Preparación del ambiente

Para llevar a cabo el desarrollo del módulo, son necesarias las siguientes herramientas: Java JDK, Python, Apache Jena Fuseki, Android Studio, Jersey, NetBeans, Visual Studio Code, Postman, Aplicación en Twitter developer.

3.2.2.1.2. Capacitaciones

Al ser el módulo de una aplicación base, es necesario el conocimiento previo sobre el funcionamiento, tecnologías y arquitectura de la misma; lo que facilitara el desarrollo del proyecto.

3.2.2.2. Planificación de fases

Las fases de la metodología Mobile-D serán descritas en la tabla 3.6; indicando el número de iteración y la descripción de las tareas a realizar.

Tabla 3.6 Planificación de fases

Fase	Iteración	Descripción
Exploración	0	Establecimiento de los interesados, definición del alcance del proyecto y análisis de los requisitos iniciales.
Inicialización	0	Accesibilidad a los servicios externos (API Twitter) y configuración de los ambientes de desarrollo y herramientas necesarias.
Producción	1	Creación de la cuenta desarrollador en la plataforma Twitter Developer Platform.
	2	Creación de una aplicación Twitter, en Developer Platform y obtención de credenciales de acceso a API v2.
	3	Generación de los wireframes y mockups del módulo de la aplicación.
	4	Creación del prototipo del módulo.
	5	Implementación de la conexión con API de Twitter v2.
	6	Configuración del entorno de desarrollo para los servicios web con Netbeans.
	7	Implementación del servicio para consultar el grupo de alumnos.
	8	Implementación del servicio para el registro del username de X

		correspondiente al alumno.
	9	Implementación del servicio para la lectura de los tweets de los alumnos.
	10	Creación del algoritmo para la identificación de tweets negativos.
	11	Implementación del servicio para el análisis y clasificación de tweets negativos.
	12	Implementación de reportes gráficos.
Estabilización	12	Corrección de errores en la lectura de datos.
	14	Corrección de errores en el registro de username de X respecto a cada alumno.
	15	Corrección de interfaces en la lectura de información.
	16	Corrección y estabilización de la detección de tweets negativos.
Pruebas del sistema	17	La realización de pruebas se llevará a cabo a través de un caso de estudio.

3.2.2.3. Diseño de la aplicación

A continuación, en la figura 3.10 se muestra la arquitectura del módulo junto con los ajustes realizados y la especificación de las tecnologías a emplear.

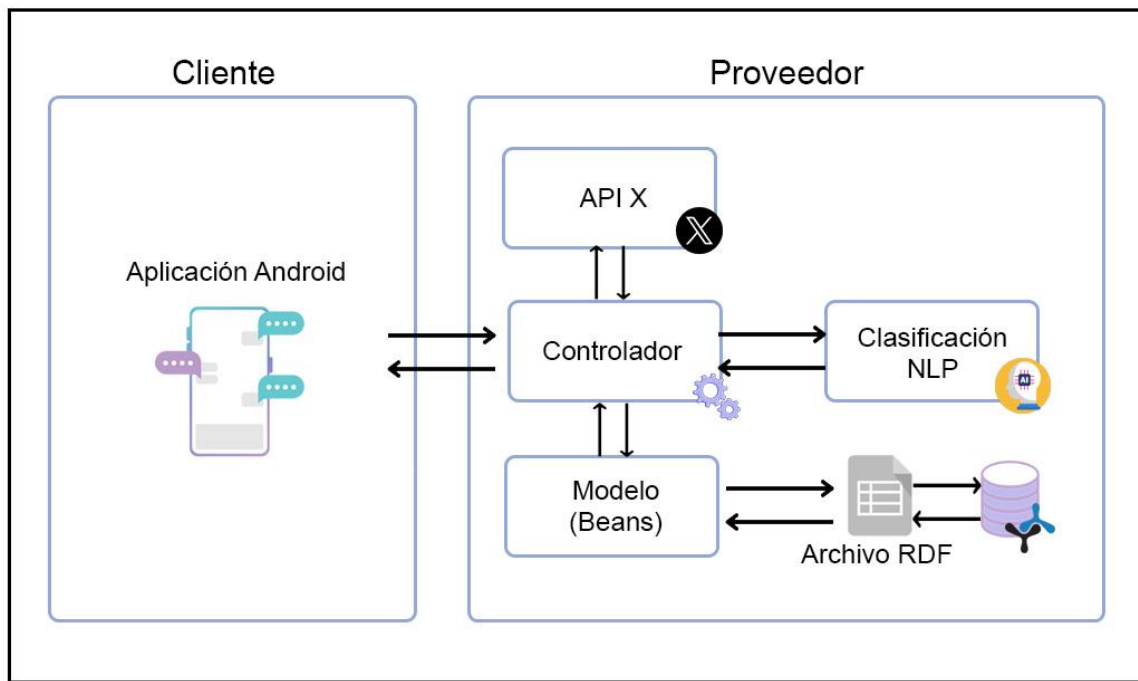


Figura 3.10 Diseño de la arquitectura para el módulo de la aplicación móvil.

3.2.2.3.1. Diagrama de casos de uso

La interacción del actor principal con el módulo de la aplicación se representa a través del diagrama de casos de uso (figura 3.11) haciendo énfasis en los requisitos funcionales.

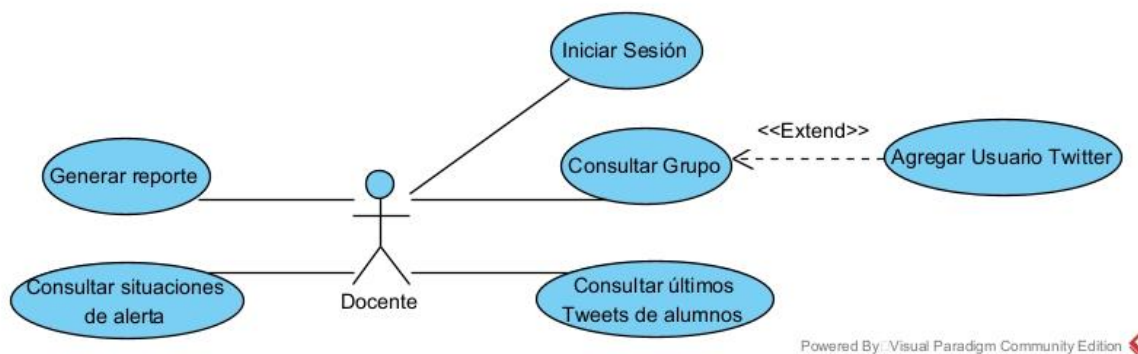


Figura 3.11 Casos de uso correspondientes al actor docente.

Así como en la aplicación base, el módulo solo es operado por un único actor, es decir, el Docente; el cual necesita autenticarse a través del inicio de sesión para poder acceder a las acciones del módulo. El docente podrá observar el listado de todo su grupo y podrá añadir el *username* de la red social X correspondiente a cada alumno, para después observar los tweets emitidos por los alumnos y las situaciones de alerta que contienen tweets malintencionados y los detalles de los mismos. Además, tendrá la opción de seleccionar la generación de un reporte.

3.2.2.4. Diseño de interfaces de usuario

En la presente sección se muestran las figuras correspondientes al diseño de interfaces del módulo (*mockups*). Cabe señalar que se continuo con la paleta de colores empleada en la aplicación base.

3.2.2.4.1. Inicio de aplicación

En la figura 3.12 se muestra la pantalla de carga al iniciar la aplicación o después del cierre de la misma.



Figura 3.12 Inicio de carga de la aplicación.

3.2.2.4.2. Inicio de sesión

Como se ha mencionado anteriormente, el docente tiene que autenticarse en la aplicación haciendo uso de un correo y contraseña; la figura 3.13 muestra la pantalla correspondiente.

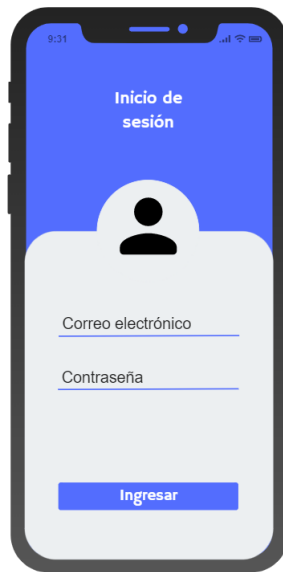


Figura 3.13 Inicio de sesión

3.2.2.4.3. Menú principal

Posteriormente a iniciar sesión en la aplicación, se muestra el menú principal (figura 3.14), donde se muestran las funcionalidades principales, junto con la opción correspondiente al módulo de ciberacoso en la parte inferior derecha.

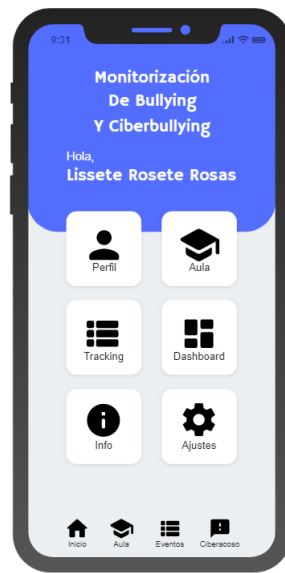


Figura 3.14 Menú principal.

3.2.2.4.4. Menú principal del módulo de ciberacoso

A continuación, se presenta la pantalla del menú de opciones con respecto al módulo de ciberacoso, con los diferentes espacios a donde accede el docente (figura 3.15).

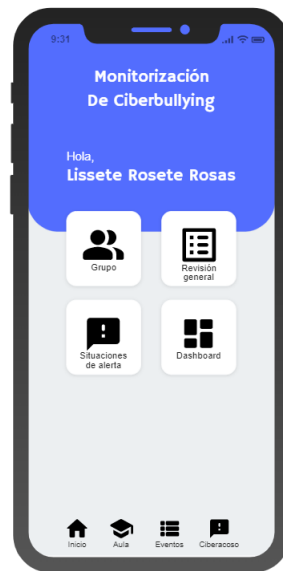


Figura 3.15 Menú principal del módulo de ciberacoso.

3.2.2.4.5. Listado de alumnos y gestión de perfiles de X

En la figura 3.16 se representa el apartado donde el docente observa el listado de su grupo de alumnos, con un botón para ingresar el *username* del perfil de X correspondiente a cada alumno y registrarlo (figura 3.17).

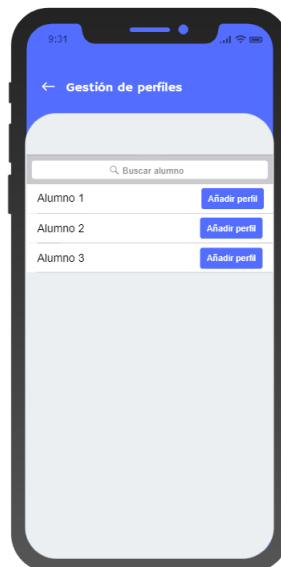


Figura 3.16 Listado de alumnos

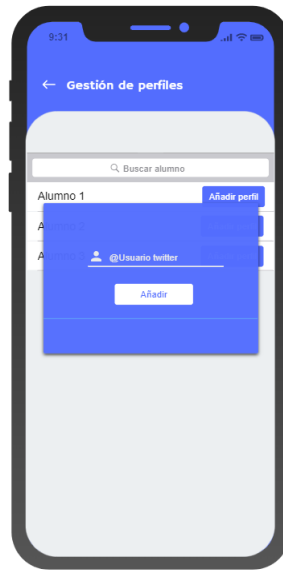


Figura 3.17 Gestión de perfil de X.

3.2.2.4.6. Revisión general

En este apartado (figura 3.18), el docente observa los últimos tweets generales realizados por su grupo de alumnos.

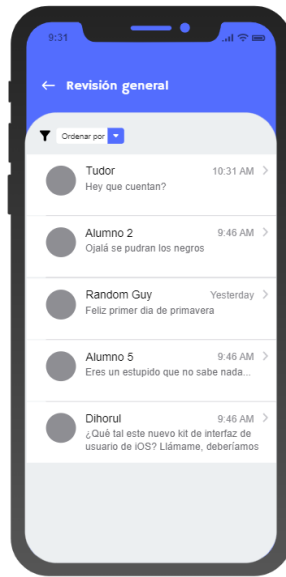


Figura 3.18 Revisión general.

3.2.2.4.7. Situaciones de alerta

En la figura 3.19 se muestra la sección de situaciones de alerta, donde se enlistarán todos aquellos tweets con contenido sensible o malintencionado, realizados por los alumnos.

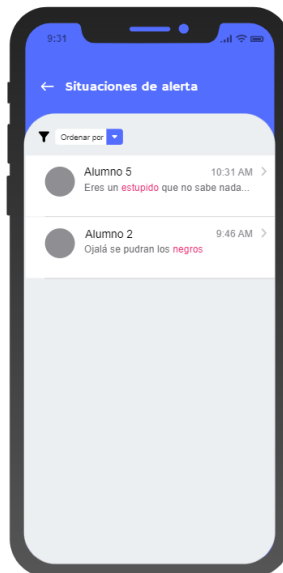


Figura 3.19 Situaciones de alerta.

3.2.2.4.8. Dashboard y reportes

Es importante tener conocimiento de aquellas estadísticas e información resumida sobre los eventos acontecidos, para que el docente pueda obtener información mejor interpretada visualmente. De igual forma la aplicación permitirá la generación de reportes con toda la información relevante (figura 3.20).



Figura 3.20 Dashboard

3.2.2.5. Diagrama de paquetes

Un diagrama de paquetes es una herramienta de modelado que se utiliza para representar la estructura de un sistema en términos de sus paquetes o módulos. Un paquete es una colección de elementos relacionados, como clases, interfaces, subpaquetes, por mencionar algunos; que proporcionan una funcionalidad común. Por lo que se representara la organización del módulo de la aplicación, comprendiendo la parte del proveedor de servicios y de la aplicación móvil.

3.2.2.5.1. Diagrama de paquetes del proveedor de servicios web

En la figura 3.21 se visualiza la estructura y contenido de los paquetes. Cabe señalar que se respetará la misma estructura que la aplicación base y las nuevas funcionalidades serán alojadas en el paquete correspondiente.

- dao: Almacena las clases de conexión al servidor Fuseki.
- dto: Almacena formateadores.
- modelo: Almacena las clases necesarias para el modelado de datos.
- wsp: Almacena las clases relacionas con los servicios REST.

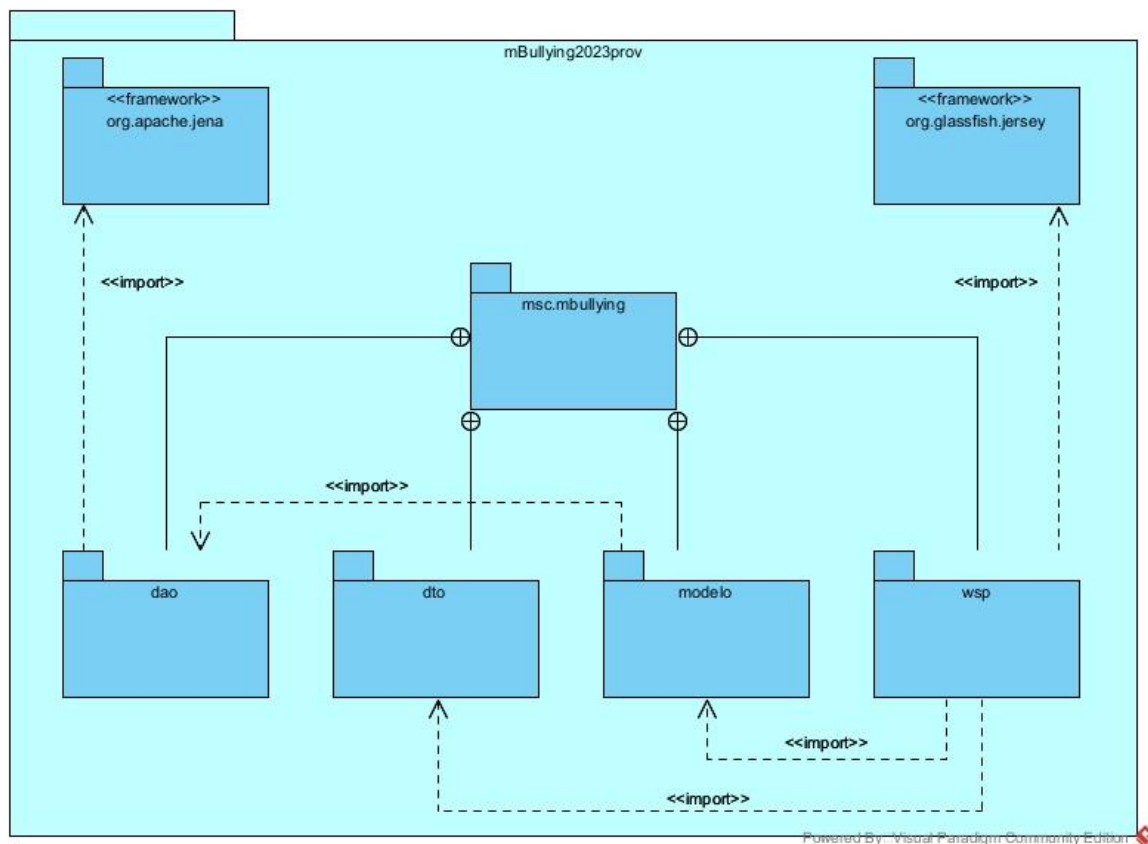


Figura 3.21 Diagrama de paquetes del proveedor de servicios web.

3.2.2.5.2. Diagrama de paquetes del módulo de la aplicación móvil

Para el caso del módulo de la aplicación móvil Android, al crear un nuevo proyecto en Android Studio, se crean varios directorios y archivos que se utilizan para estructurar y organizar el código de la aplicación. Además, se agregan carpetas necesarias para la mejor estructuración del sistema. La distribución de los paquetes se encuentra representada en la figura 3.22.

- activities: Almacena las clases que representan una pantalla o una interfaz de usuario. Cada actividad tiene una o varias ventanas de vista o fragmentos.
- fragments: Almacena las clases que definen los fragmentos de la aplicación.
- interfaces: Almacena las interfaces utilizadas para la comunicación entre fragments y el procesamiento de los datos consumidos por los servicios web.
- adapters: Almacena la configuración de las encargadas de generar las listas dinámicas de información para su visualización.
- Conexión X API v2: Almacena la configuración para realizar la conexión con la API de Twitter y obtener datos como, por ejemplo, los tweets.
- jnLibs: Almacena aquellas bibliotecas a emplear.
- res: (acrónimo de recursos) es una carpeta importante que se utiliza para almacenar todos los recursos de la aplicación, como imágenes, archivos de sonido, diseños de interfaz de usuario, iconos, valores de cadena, estilos, animaciones, etc.

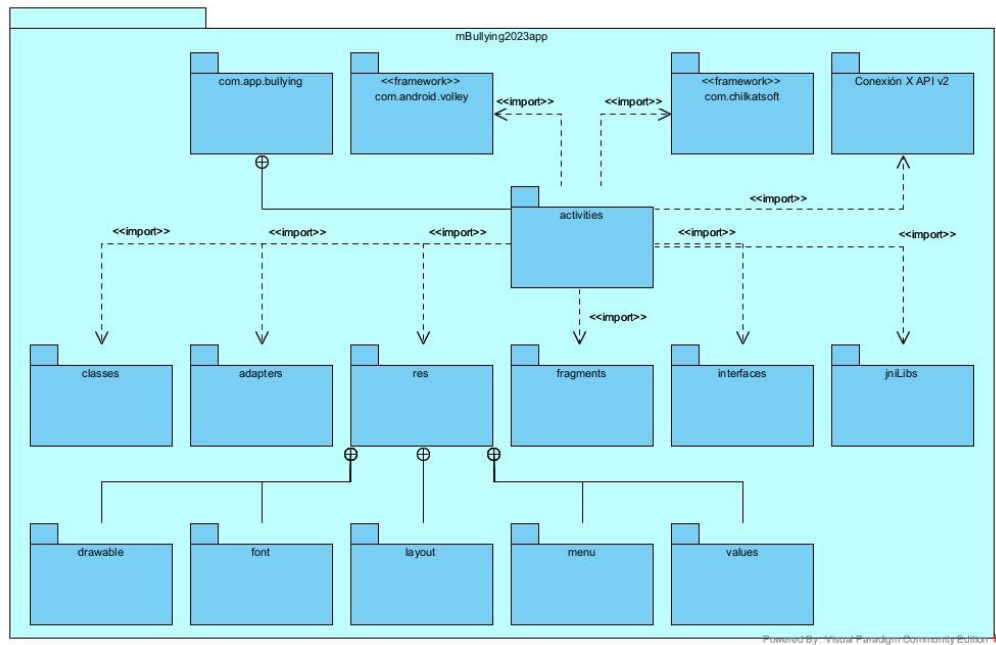


Figura 3.22 Diagrama de paquetes del módulo de la aplicación móvil.

3.2.2.6. Diagramas de clases

A continuación, en la figura 3.23 se muestra el diagrama de clases correspondiente al módulo de la aplicación móvil.

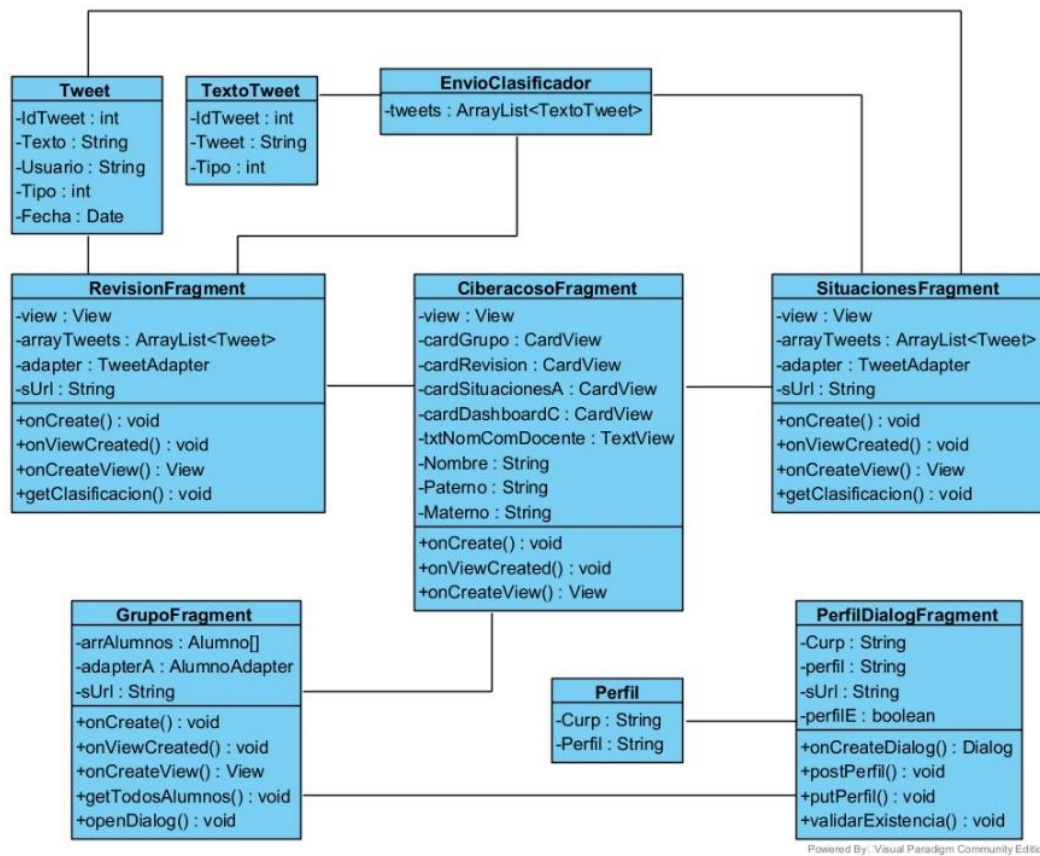


Figura 3.23 Diagrama de clases correspondiente al módulo de la aplicación móvil.

3.2.3. Producción y Estabilización

En esta fase se lleva a cabo el desarrollo del módulo de la aplicación móvil, se repite iterativamente hasta implementar todas las funcionalidades recolectadas en los requisitos recolectados en las fases anteriores.

3.2.3.1. Aplicación en Twitter Developer

Para poder realizar la conexión con la API de Twitter, son necesarias las credenciales otorgadas a través de una aplicación en el portal para desarrolladores de X. Para esto, es necesaria la creación de una cuenta de desarrollador a través de un formulario donde se solicita información básica del desarrollador y la creación de una aplicación

en dicho portal; para esto, una vez verificada la cuenta, se crea una nueva aplicación de Twitter y el proceso se encuentra dividido en 4 secciones, la información básica que aborda información personal, el uso previsto que es donde se expone explícitamente cuales son los motivos o con que finalidad se busca acceder a la API de Twitter; la revisión, donde si se desea editar algún campo es posible regresar al formulario anterior y por último la sección donde se aceptan los términos y condiciones (figura 3.24).

The screenshot shows the 'Basic info' section of the Twitter Developer Portal. The form is titled 'Basic info' and is part of a 4-step process. It contains the following fields and options:

- What's your name?** (This is permanent and can't be changed.): LisRR
- What country are you based in?**: Mexico
- What's your current coding skill level?** (optional): Some experience
- Want updates and access to more resources? (optional)**: ☒ Yes, send updates.

The form has 'Back' and 'Next' buttons at the bottom. The left sidebar shows the 'Developer Portal' logo and a '#TheBasics' section with instructions. The footer includes links for Privacy, Cookies, Terms, and Developer Policy, along with social media links and a date/time display.

Figura 3.24 Previsualización del formulario para la creación de aplicación.

Posterior a la verificación y aceptación de la aplicación se procede con la generación del “Bearer Token” (figura 3.25), el cual es un tipo de token de autenticación utilizado en sistemas de seguridad de aplicaciones web y API RESTful. Este token se utiliza para autenticar solicitudes de un cliente al servidor, permitiendo así el acceso a los recursos protegidos.

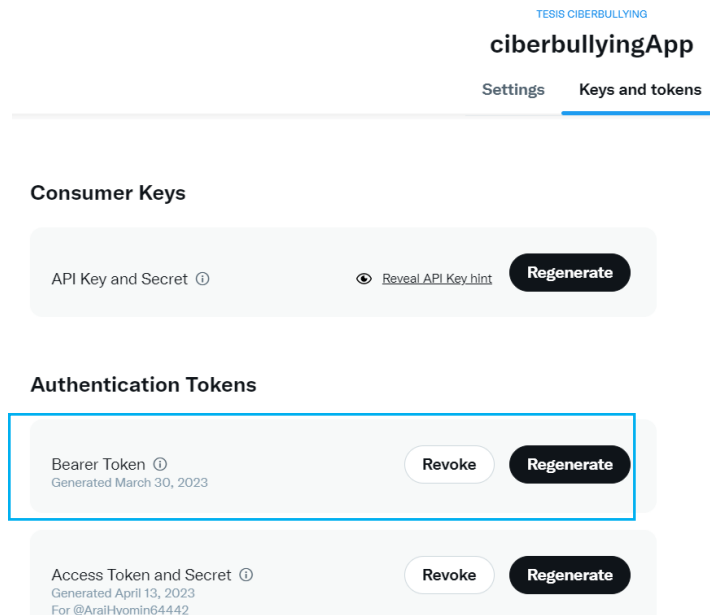


Figura 3.25 Credenciales para acceso a la API Twitter v2.

3.2.3.2. Implementación de la conexión con la API de Twitter

Para realizar las pruebas y el correcto funcionamiento de las solicitudes a la API de Twitter, se realizó una aplicación móvil en Android Studio. Como primer punto se requirió de una biblioteca otorgada por *Chilkat Software*, la cual proporciona una amplia gama de herramientas y funcionalidades como, por ejemplo, la comunicación con servidores mediante protocolos de transferencia seguros como SFTP o HTTPS y también incluye herramientas de análisis de XML y JSON.

Por otro lado, la API de Twitter funciona a través de *endpoints*, los cuales son URL que permiten acceder a los recursos o funcionalidades de la plataforma. Cada *endpoint* de la API de Twitter corresponde a una acción o consulta específica y se compone de una URL que comienza con el prefijo "https://api.twitter.com/" y se completa con un sufijo específico.

Primeramente, se necesita del *username* del usuario de Twitter para obtener su información principal, por lo que una vez ingresado, se ejecuta el método “Buscar” (listado 3.1) donde se forma el *endpoint* correspondiente y se envía al método de “EjecutarConsulta” (listado 3.2) el cual es el método general para realizar las peticiones correspondientes a la API de Twitter y obtener el cuerpo de la respuesta en formato JSON.

Listado 3.1 Método "Buscar" a través de username de usuario

```

1 public void Buscar(View view){
2     //Recuperar lo del input
3     txtUsername = findViewById(R.id.txtUsername);
4     //Asignar a variable String la información del input username
5     String sUsername = txtUsername.getText().toString();
6     String urlUserByUsername = "https://api.twitter.com/2/users/by/username/" + sUsername;
7     response = consulta.EjecutarConsulta(urlUserByUsername);
8     mostrarDatos(response);
9 }

```

Listado 3.2 Método general para ejecutar consultas

```

1 public JSONObject EjecutarConsulta(String url){
2     //CkHttp: Clase para enviar solicitudes HTTP y recibir respuestas del servidor.
3     CkHttp http = new CkHttp();
4     http.DnsCacheClear();
5     boolean success;
6
7     //Acceso a través de Baerer Token
8     http.put_AuthToken("AAAAAAAAAAAAAAAAAAAAAB6UmQEAAAAAASM7cwCneBEDmZ0jI6GF0RLIpWY%3
9         DL760OpU8zCPLrhBuUrmCtYYYWRxbVPCiWOECFvq34J082R5j0H");
10
11     //Clase para construir cadenas.
12     CkStringBuilder sbResponseBody = new CkStringBuilder();
13     //Envía una solicitud HTTP GET para una URL
14     success = http.QuickGetSb(url, sbResponseBody);
15
16     if (success == false) {
17         respuesta = "Error al ejecutar consulta " + http.lastErrorText();
18         Log.i(TAG, respuesta);
19     }
20
21     CkJsonObject jResp = new CkJsonObject();
22     jResp.LoadSb(sbResponseBody);
23     jResp.put_EmitCompact(false);
24     JSONObject obj = null;
25     try {
26         obj = new JSONObject(jResp.emit()); //Convierte la respuesta en objeto JSON

```

```

27     } catch (JSONException e) {
28         throw new RuntimeException(e);
29     }
30
31     //Código para conocer el status de la solicitud o los errores encontrados.
32     int respStatusCode = http.getLastStatus();
33     Log.i(TAG, "Response Status Code = " + String.valueOf(respStatusCode));
34     if (respStatusCode >= 400) {
35         Log.i(TAG, "Response Header:");
36         Log.i(TAG, http.lastHeader());
37         Log.i(TAG, "Failed.");
38     }
39     String detail, title, resource_type, parameter, value, v_type;
40     int i = 0;
41     int count_i = jResp.SizeOfArray("errors");
42     while (i < count_i) {
43         jResp.put_I(i);
44         detail = jResp.stringOf("errors[i].detail");
45         title = jResp.stringOf("errors[i].title");
46         resource_type = jResp.stringOf("errors[i].resource_type");
47         parameter = jResp.stringOf("errors[i].parameter");
48         value = jResp.stringOf("errors[i].value");
49         v_type = jResp.stringOf("errors[i].type");
50         i = i + 1;
51     }
52     return obj; //El método retorna el objeto JSON.
53 }
54
55 static {
56     System.loadLibrary("chilkat");
57 }

```

El método “obtenerTweets” (listado 3.3) genera el array de tweets obtenidos a través del objeto Tweet, agregando el ID del tweet y su texto correspondiente.

Listado 3.3 Método para obtener los tweets del usuario

```

1 public void ObtenerTweets(String urlTweets) throws JSONException {
2     responseT = consulta.EjecutarConsulta(urlTweets);
3     //List<Tweet> items = new ArrayList<>();
4     ArrayList<Tweet> tweetsList = new ArrayList<>();
5     JSONArray array = responseT.getJSONArray("data");
6     for (int i = 0; i<array.length(); i++){
7         Tweet t = new Tweet("", "");
8         JSONObject obj = array.getJSONObject(i);
9         t.setText(obj.getString("text"));
10        t.setId(obj.getString("id"));
11        tweetsList.add(t);
12    }
13    TweetListAdapter adapterT = new TweetListAdapter(this,
14                                                    R.layout.adapter_view_layout, tweetsList);
15    listTweets.setAdapter(adapterT);
16    listTweets.setOnItemClickListener(new AdapterView.OnItemClickListener() {
17        @Override
18        public void onItemClick(AdapterView<?> parent, View view, int position, long id) {
19            Object obj = listTweets.getAdapter().getItem(position);
20            Tweet tw = new Tweet("", "");
21            tw = (Tweet) obj;
22            tw.getId();
23            String valueId = tw.getId();
24            Log.i(TAG, valueId);
25            Intent confirm = new Intent(MainActivity.this, TweetDetails.class);
26            confirm.putExtra("value", valueId);
27            startActivity(confirm);
28        }
29    });
30 }

```

3.2.3.3. Algoritmo de aprendizaje y clasificación

En esta sección se presenta la metodología que se estableció para llevar a cabo el análisis de los modelos predictivos para identificar los tweets negativos y la implementación del modelo predictor. La metodología se ve reflejada gráficamente en la figura 3.26 y se compone de las etapas de recolección de datos, generación de un corpus, etiquetado manual de documentos, preprocesamiento de los documentos, extracción de características, ajuste de parámetros para los modelos predictivos y la experimentación junto con la evaluación de los modelos. A continuación, se explican detalladamente cada una de las etapas mencionadas.



Figura 3.26 Metodología para el análisis de los modelos predictivos.

- **Recolección de datos**

En esta etapa, se obtuvieron datos que se descargaron de la plataforma X. Para dicha recolección se utilizó un script escrito en Python que emplea la biblioteca snsrape; el procedimiento para recolectar los documentos (tweets/posts), fue el siguiente:

- Se realizó una consulta principal con las palabras clave en la presencia del ciberacoso, dichas palabras fueron tomadas de la bolsa de palabras recabada anteriormente. Además, se realizaron consultas de posts aleatorios.
- Las consultas realizadas se limitaron a recabar tweets solamente escritos en idioma español, cabe mencionar que debido a la esencia de las palabras clave utilizadas, la mayoría de los tweets contemplaron agresiones/blasfemias más generales en el habla hispana y así mismo, propias del español mexicano.
- Los documentos descargados se encontraban en formato JSON (acrónimo de JavaScript Object Notation, notación de objeto de JavaScript) y posteriormente se almacenaron en archivos de valores separados por comas, obteniendo una cantidad de 10 mil documentos o posts de acuerdo a la plataforma X.

Para la generación del corpus, de los 10 mil posts recolectados se tomó una muestra aleatoria de 2500, que conformarían los documentos a etiquetar.

- Etiquetado

El aprendizaje supervisado es un tipo de técnica de aprendizaje automático en la que se entrena a un modelo utilizando un conjunto de datos etiquetado, es decir, un conjunto de ejemplos de entrada junto con las respuestas deseadas. Por lo que, se llevó a cabo el etiquetado manual de los documentos que conforman el corpus, se dio lectura detallada a cada uno y se le asignó la etiqueta o categoría que mejor correspondiera al sentimiento expuesto en el texto. Las etiquetas que podían ser asignadas fueron las siguientes: “Ciberbullying”, “No Ciberbullying” y “No Relacionado”. Dichas etiquetas o categorías quedaron sujetas a un conjunto de reglas que fueron establecidas (figura 3.27), las cuales se exponen a continuación:

- **Cyberbullying.** Un documento es etiquetado en esta categoría si contiene:
 - Por lo menos una grosería dirigida a una persona o varias personas.
 - Mensajes que contengan palabras hirientes dirigidas a una o varias personas.
 - Mensajes que inciten a la discriminación.
 - Mensajes que insulten a una persona o varias personas.
 - Mensajes que amenacen a una persona o varias personas.
 - Mensajes que denigren a un sexo en específico.
 - Maldiciones o burlas en contra de una persona o varias personas.
 - Mensajes que tengan como objetivo ridiculizar a una persona o varias personas.
 - Mensajes que contengan un apodo despectivo hacia un individuo o individuos.
 - Mensajes que contengan emojis relacionados con el ciberacoso
(🤪 😡 🙄 🐼 🧟 🧛 🧑 🧔 🧒 🧓 🧖 🧜 🧝 🧚 🧞 🧛 🧜 🧝 🧚 🧞 🧛 🧜 🧝 🧚 🧞)
- **No Cyberbullying.** Un documento se considera en esta categoría si al leerse se identifican:
 - Mensajes que contengan una o varias groserías que no estén dirigidas hacia ninguna persona.
 - Mensajes que adulen a una o varias personas.
 - Mensajes que demuestren apoyo hacia una o varias personas.
 - Mensajes cuya finalidad sea alentar o animar a uno o varios individuos.
 - Mensajes que tengan como objetivo defenderse o defender a otra/as personas; sin intención de insultar.
- **No relacionado.** Un documento se etiqueta como no relacionado si contiene:
 - Mensajes que no tengan relación con los puntos anteriores, como noticias, campañas de marketing o publicidad.
 - Mensajes donde únicamente coloquen hashtags o se etiqueten personas
 - Mensajes que realicen invitaciones a conferencias, concursos, programas de radio, entre otros.
 - Mensajes que contengan imágenes o enlaces.

Figura 3.27 Reglas de clasificación

Una vez realizado el etiquetado de los 2500 documentos seleccionados, la cantidad de documentos categorizados en las diferentes clases concluyó de la siguiente manera:

- Cyberbullying: 616
 - No cyberbullying: 495
 - No relacionado: 1389
-
- Preprocesamiento de textos

Ya que los documentos que fueron descargados contienen diversos elementos en el texto, como símbolos, emoticones, hashtags, imágenes, videos, enlaces, entre muchos otros; es necesaria la eliminación de elementos que no contribuyen o que no aportan información relevante para el tema de estudio, en este caso, identificar mensajes ofensivos. Un ejemplo claro de los elementos no relevantes son las palabras vacías (Stop Words) por ejemplo, conjunciones, preposiciones, artículos, etc.

Después de analizar los elementos de importancia en los documentos, se desarrollaron scripts en Python que permitieron la limpieza de cada uno de los documentos; se eliminaron o removieron los siguientes elementos:

- Se eliminaron los acentos y números.
- Caracteres especiales tales como ". \$ % & / () = ? , ; .
- Direcciones de internet, las cuales comienzan con el texto "http".
- Emoticones no relacionados con el cyberbullying.
- Stopwords o palabras vacías.

El objetivo de este paso es mejorar la calidad de las características y al mismo tiempo reducir la dificultad del proceso de clasificación.

- Extracción de características

La extracción de características en documentos se refiere al proceso de identificar y representar las características clave o información relevante contenida en un

documento de texto. Para ello se requiere que los documentos se encuentren como datos estructurados, es decir, que se vectoricen. La vectorización de un documento implica convertir un documento de texto en una representación numérica (vector). Se empleó la técnica TF-IDF (TF-IDF del inglés Term Frequency – Inverse Document Frequency, Frecuencia de Término – Frecuencia Inversa), la cual elimina los términos más comunes y extrae solo los términos más relevantes del corpus. En esta técnica el valor de cada token aumenta proporcionalmente al número de veces que una palabra aparece en el documento, pero es compensada por la frecuencia de la palabra en la colección de documentos, lo que permite manejar el hecho de que algunas palabras son generalmente más comunes que otras.

Aplicando la técnica TF-IDF sobre el corpus, se obtuvo una matriz dispersa de 2500 documentos y un total de 11191 palabras.

- Ajuste de parámetros para los modelos predictivos

Existen varios métodos de aprendizaje automático y en este caso, se contemplaron métodos de aprendizaje supervisado, en el que se entrena a un modelo utilizando un conjunto de datos etiquetado. Cada ejemplo de entrenamiento consta de una entrada (características) y una etiqueta (la salida deseada).

Para la identificación de la posible presencia de ciberacoso, se consideraron tres diferentes tipos de métodos de aprendizaje supervisado: Máquina de Vector Soporte (SVM del inglés Support Vector Machine), Bosque aleatorio (RF del inglés Random Forest) y Perceptrón Multicapa (MLP del inglés Multilayer Perceptron).

Debido a que cada uno de los métodos contienen sus propios parámetros, en lugar de adivinar cuáles son los mejores valores para estos hiperparámetros se optó por emplear el método de búsqueda por rejilla, también conocido como búsqueda en cuadrícula o "grid search" en inglés; lo que permitió encontrar la mejor combinación de hiperparámetros para el modelo, en la tabla 3.7 se muestra la configuración acorde a cada método de clasificación.

Tabla 3.7 Configuración de hiperparametros a través del método de búsqueda por rejilla.

Vectorizador	Clasificador		
	SVM	RF	MLP
TF-IDF	kernel: 'rbf' gamma: 2.3734	criterion: 'gini' max_depth:100 n_estimators: 150	activation: 'tanh' alpha: 0.05 hidden_layer_sizes: (100,) learning_rate: 'adaptive' solver: 'adam'

- Experimentación y evaluación

En esta etapa se llevó a cabo la comparación del desempeño de los diferentes métodos de clasificación empleando la vectorización TF-IDF. Las métricas a tomar en cuenta fueron la precisión (precision), la exhaustividad (recall) y F1-score. Los resultados obtenidos se exponen en la tabla 3.8.

Tabla 3.8 Desempeño de los clasificadores para la vectorización TF-IDF.

Clases	Clasificador	Precision	Recall	F1-Score
Ciberbullying	SVM	0.57	0.37	0.45
	RF	0.74	0.27	0.39
	MLP	0.59	0.35	0.44
No ciberbullying	SVM	0.66	0.42	0.52
	RF	0.71	0.53	0.61
	MLP	0.62	0.36	0.45
No relacionado	SVM	0.74	0.94	0.83
	RF	0.71	0.98	0.82
	MLP	0.69	0.93	0.79

Se observa que el desempeño de los clasificadores es bajo para las clases ciberbullying y no ciberbullying, debido al desbalance de las clases, pues como previamente se mencionó, dichas clases presentaban una minoría de documentos en comparación con la clase “No relacionado”. El desbalanceo afecta negativamente el

rendimiento del modelo, ya que el algoritmo puede tener dificultades para aprender la clase minoritaria debido a la falta de instancias.

Existen algunas estrategias comunes para abordar el desbalanceo de clases en el aprendizaje automático, para este caso en particular se optó por emplear SMOTE que es un acrónimo que significa "Synthetic Minority Oversampling Technique". SMOTE es una técnica de sobre muestreo que se utiliza para generar ejemplos sintéticos de la clase minoritaria, lo que ayuda a equilibrar las proporciones de clases en el conjunto de datos sin necesidad de reducir el tamaño de la clase mayoritaria.

Después de aplicar la técnica correspondiente para balancear las clases, nuevamente se llevó a cabo la clasificación para cada uno de los diferentes métodos y los resultados obtenidos se reflejan en la tabla 3.9; observando que se obtuvieron mejores desempeños en las métricas contempladas.

Tabla 3.9 Desempeño de los clasificadores para la vectorización TF-IDF con técnica SMOTE.

Clases	Clasificador	Precision	Recall	F1-Score
Ciberbullying	SVM	1.00	0.73	0.84
	RF	0.95	0.76	0.84
	MLP	0.93	0.91	0.92
No ciberbullying	SVM	0.99	0.84	0.91
	RF	0.88	0.90	0.89
	MLP	0.94	0.95	0.94
No relacionado	SVM	0.70	0.99	0.82
	RF	0.80	0.94	0.87
	MLP	0.90	0.91	0.91

El clasificador que obtuvo mejor desempeño para la vectorización TF-IDF fue MLP, pues presenta mejores métricas y los métodos de clasificación SVM y RF, presentan resultados similares entre sí. De este modo, el modelo clasificador de los tweets negativos emplea Multi-Layer Perceptron.

3.2.3.4. Creación de API Python para análisis de tweets

Para la implementación del modelo clasificador de los tweets, se diseñó una API en Python con la ayuda del framework web Flask, el cual es muy flexible y permite construir rápidamente servicios web RESTful. Además del uso de un entorno virtual.

Una parte importante del proceso para clasificar los datos, es la limpieza del texto (mencionado anteriormente en la etapa de preprocesamiento de textos), para lo cual se empleó una clase en Python que permita la eliminación de aquellos caracteres y/o palabras innecesarias (listado 3.4).

Listado 3.4 Clase de limpieza de documentos.

```

1 class TweetClean:
2
3     #Limpiar el texto del tweet
4     def cleanTweet(self, text):
5         text = self.replaceVocals(text)
6         text = self.removeComma(text)
7         text = self.removeDots(text)
8         text = self.removeSymbols(text)
9         text = self.removeParenthesis(text)
10        text = self.removeBrackets(text)
11        text = self.removeEmojis(text)
12        text = self.removeSpaces(text)
13        text = self.removeLinks(text)
14        text = self.removeNumbers(text)
15        text = self.removeStopWords(text)
16        return text
17
18    def replaceVocals(self, text):
19        replacements = (
20            ("á", "a"),
21            ("é", "e"),
22            ("í", "i"),
23            ("ó", "o"),
24            ("ú", "u"),
25        )
26        for a, b in replacements:
27            text = text.replace(a, b).replace(a.upper(), b.upper())
28        return text
29
30    def removeSpaces(self, text):
31        text = text.strip()
32        text = text.replace("\n", "")
33        return text
34
35    def removeComma(self, text):
36        text = text.replace(",", "")
37        return text
38
39    def removeDots(self, text):
40        text = text.replace(".", "")
41        text = text.replace("..", "")
42        text = text.replace("...", "")
43        return text
44
```

```

46 def removeSymbols(self, text):
47     text = text.replace("&", "")
48     text = text.replace("?", "")
49     text = text.replace("'", "")
50     text = text.replace("/", "")
51     return text
52
53 def removeParenthesis(self, text):
54     text = text.replace('(', '').replace(')', '')
55     return text
56
57 def removeBrackets(self, text):
58     text = text.replace('[', '').replace(']', '')
59     return text
60
61 def removeEmojis(self, text):
62     regex_pattern = re.compile(pattern = "["
63     u"\U0001FAE0"
64     u"\U0001FAF6"
65     u"\U000026BD"
66     u"\U00002639"
67     u"\U0001FA79"
68     u"\U000026A1"
69     u"\U00002700-\U00002709" #dingbats
70     u"\U0000270B-\U000027BF"
71     u"\U0001F600-\U0001F64F" # emoticons
72     u"\U0001F300-\U0001F345" # symbols & pictographs
73     u"\U0001F347-\U0001F40C"
74     u"\U0001F40E-\U0001F42C"
75     u"\U0001F42F-\U0001F436"
76     u"\U0001F438-\U0001F43C"
77     u"\U0001F43E-\U0001F449"
78     u"\U0001F44B-\U0001F47F"
79     u"\U0001F481-\U0001F4A5"
80     u"\U0001F4A7-\U0001F4A8"
81     u"\U0001F4AB-\U0001F529"
82     u"\U0001F52C-\U0001F594"
83     u"\U0001F596-\U0001F5FF"
84     u"\U0001F680-\U0001F6FF" # transport & map symbols
85     u"\U0001F1E0-\U0001F1FF" # flags (iOS)
86     u"\U0001F900-\U0001F920" # supplemental symbols and pictographs
87     u"\U0001F923-\U0001F925"
88     u"\U0001F927-\U0001F92B"
89     u"\U0001F92D-\U0001F92D"
90     u"\U0001F92F-\U0001F9FF"
91     | | | | | "]" +, flags = re.UNICODE)
92     return regex_pattern.sub(r'',text)
93
94 def removeLinks(self, text):
95     matches = re.findall(r'http\S+', text)
96     for match in matches:
97         text = text.replace(match, '')
98     return text
99
100 def removeNumbers(self, text):
101     text = re.sub(r'[0-9]+', '', text)
102     return text
103
104 def removeStopWords(self, text):
105     stop_words = set(stopwords.words('spanish'))
106     text = ' '.join([word for word in text.split() if word.lower() not in stop_words])
107     return text

```

El modelo clasificador de tweets (listado 3.5) contempla parte del procedimiento descrito anteriormente, pues contiene la vectorización TF-IDF del corpus, el balanceo de clases y el método de aprendizaje supervisado seleccionado (Multi-Layer Perceptron) con el ajuste de sus determinados parámetros y el método para predecir la etiqueta de una nueva entrada.

Listado 3.5 Clase con el modelo predictor

```

1 class Clasificador:
2     transformer = None
3     clf = None
4
5     def __init__(self):
6         self.entrenador()
7         print("lisuya piciosa")
8
9     def entrenador(self):
10        df = pd.read_csv("Corpus_cleaned.csv")
11        corpus = df.iloc[:, 1]
12        labels = df.iloc[:, 2]
13
14        #Vectorización
15        self.transformer = TfidfVectorizer()
16        corpus = corpus.fillna(' ')
17        tfidf = self.transformer.fit_transform(corpus)
18        self.transformer.get_feature_names_out() # Palabras
19        X = tfidf.toarray()
20
21        le = preprocessing.LabelEncoder()
22        le.fit(labels)
23        y = le.transform(labels)
24
25        #Para el balanceo de clases
26        smote = SMOTE(random_state=42)
27        X_sm, y_sm = smote.fit_resample(X, y)
28        unique, counts = np.unique(y_sm, return_counts=True)
29
30        #Usa el 80% para entrenamiento
31        X_train, X_test, y_train, y_test = split(X_sm, y_sm, train_size=0.8, random_state=42)
32
33        #Creación del modelo MLP
34        self.clf = MLPClassifier(max_iter=100, activation= 'tanh', alpha= 0.05,
35                                hidden_layer_sizes= (100,), learning_rate= 'adaptive', solver= 'adam')
36        self.clf.fit(X_train, y_train)
37
38    def clasificacion(self, tweet):
39        #test
40        vectTweet = self.transformer.transform(np.array([tweet]))
41
42        prediction = self.clf.predict(vectTweet)
43        return 0 if prediction[0]==0 else 1
44

```

Para el correcto funcionamiento de la API se requiere del ruteo que permite responder a solicitudes GET/POST devolviendo un mensaje JSON. De este modo cada tweet de

entrada pasa por el proceso de limpieza de datos y por el modelo de clasificación asignando la etiqueta correspondiente de acuerdo al modelo.

Listado 3.6 Ruteo de las solicitudes

```

1  from tweets_clean import TweetClean
2  from clasificador import Clasificador
3  from flask import Flask, jsonify, request
4  import json
5
6
7  app = Flask(__name__)
8
9  cl = Clasificador()
10
11  @app.route('/')
12  def root():
13      return "Home"
14
15  @app.route("/clasificacion/tweet/<tweet>")
16  def get_clasificacion(tweet):
17      tc = TweetClean()
18      tweetClean = tc.cleanTweet(tweet)
19      tipo = cl.clasificacion(tweetClean)
20      tweetAnalisis = {"tipo": tipo, "tweet": tweet}
21      query = request.args.get('query')
22      if query:
23          tweetAnalisis["query"] = query
24      return jsonify(tweetAnalisis), 200
25
26  @app.route("/clasificacion/tweets", methods=["POST"])
27  def post_clasificacion():
28      try:
29          data = request.get_json()
30          datosOk = str(data).replace('\n', '')
31          print(datosOk)
32
33          datos = json.loads(datosOk)
34          contador = 0
35          for i in datos["tweets"]:
36              tweet = datos["tweets"][contador]["tweet"]
37              tc = TweetClean()
38              tweetClean = tc.cleanTweet(tweet)
39              tipo = cl.clasificacion(tweetClean)
40              datos["tweets"][contador]["tipo"] = tipo
41              contador = contador + 1
42          return jsonify(datos), 200
43      except Exception as error:
44          print("An exception occurred:", error)
45

```

3.2.3.5. Métodos de escritura de datos

A continuación, se muestran los métodos para la consulta, inserción y modificación de datos correspondientes para el perfil de la red social X (utilizando SPARQL para todos los casos); el listado 3. Muestra la consulta del *username* de X y ya que los perfiles serán correspondientes a cada alumno registrado en el grupo, en la base de tripletas se realiza el registro del *username* en relación al *curp* del alumno (listado 3.) y el método *update* (listado 3.) permite la actualización del *username* del perfil en X.

Listado 3.7 Método para la consulta del *username* de la red social X correspondiente al alumno.

```

1 public boolean search(String sCurp) throws Exception {
2     boolean bRet = false;
3     ArrayList arrayResult = null, linea = null;
4
5     sQuery = "PREFIX foaf: <http://xmlns.com/foaf/0.1/>"
6             + "SELECT * WHERE {"
7             + "?perfil foaf:curpUsuario ?a. "
8             + "?perfil foaf:perfil ?b."
9             + "    FILTER(?a = 'X' + sCurp + '')"
10            + "}";
11
12     if (oData == null) {
13         oData = new AccesoDatos();
14         arrayResult = oData.readQueryPerfil(sQuery);
15     } else {
16         arrayResult = oData.readQueryPerfil(sQuery);
17     }
18     if (arrayResult != null && arrayResult.size() > 0) {
19         List<Perfil> rs = arrayResult;
20
21         this.setCurp(rs.get(0).getCurp());
22         this.setPerfil(rs.get(0).getPerfil());
23         bRet = true;
24     }
25     return bRet;
26 }

```

Listado 3.8 Método para el registro del perfil de la red social X.

```

1 public void create() throws Exception {
2
3     sQuery = "PREFIX foaf: <http://xmlns.com/foaf/0.1/>"
4             + "PREFIX :<http://localhost:8080/mBullying2022prov/"
5             + "mbullying/crud/perfiles/buscar?txtCurp=>"
6             + "INSERT DATA {"
7             + "    :X" + Curp
8             + " foaf:curpUsuario 'X" + Curp + "';"
9             + "    foaf:perfil '" + Perfil + "';"
10            + "} ";
11
12    if (oData == null) {
13        oData = new AccesoDatos();
14        oData.createQuery(sQuery);
15    } else {
16        oData.createQuery(sQuery);
17    }
18 }

```

Listado 3.9 Método para la modificación del perfil de la red social X.

```

1 public void update() throws Exception {
2
3     sQuery = "PREFIX foaf: <http://xmlns.com/foaf/0.1/>"
4             + "PREFIX :<http://localhost:8080/mBullying2022prov/"
5             + "mbullying/crud/perfiles/buscar?txtCurp=>"
6             + "DELETE {"
7             + "    :X" + Curp + " foaf:curpUsuario ?a;"
8             + "    foaf:perfil ?b;"
9             + "}"
10            + "INSERT {"
11            + "    :X" + Curp + " foaf:curpUsuario 'X" + Curp + "';"
12            + "    foaf:perfil '" + Perfil + "';"
13            + "}"
14            + "WHERE {"
15            + "    :X" + Curp + " foaf:curpUsuario ?a;"
16            + "    foaf:perfil ?b;"
17            + "}"
18
19    if (oData == null) {
20        oData = new AccesoDatos();
21        oData.updateData(sQuery);
22    } else {
23        oData.updateData(sQuery);
24    }
25 }

```

3.2.3.6. Métodos para los servicios web

Al igual que la aplicación móvil base, los servicios web se encuentran basados en las clases del marco de trabajo Jersey, a continuación, se muestran ejemplos de los métodos GET, POST Y PUT (listados 3.10, 3.11 y 3.12).

Listado 3.10 Método para la lectura de información del username de X.

```

1  @GET
2  @Path("/perfiles/buscar")
3  @Produces(MediaType.APPLICATION_JSON)
4  public Response getInfoPerfil(@QueryParam("txtCurp") String sCurp)
5  {
6      throws Exception {
7          String sCadJson = "";
8          Response response = null;
9          ObjectMapper mapper = new ObjectMapper();
10
11      try {
12          if (sCurp.isEmpty()) {
13              response = Response.notAcceptable(null).build();
14          } else {
15              PerfilDTO perfilDTO = service.buscarPerfil(sCurp);
16
17              if (perfilDTO != null) {
18                  sCadJson = mapper.writeValueAsString(perfilDTO);
19                  response = Response.ok(sCadJson,
20                      MediaType.APPLICATION_JSON).build();
21              } else {
22                  response = Response.ok("{\"Error\":\"NO SE ENCONTRÓ\"}",
23                      MediaType.APPLICATION_JSON).build();
24              }
25          }
26      } catch (Exception e) {
27          response = Response.serverError().entity(
28              "{\"Error\":\"OCURRIÓ ALGO DURANTE LA BUSQUEDA\"}").build();
29          e.printStackTrace();
30      }
31      return response;
32  }
33
34
35  @GET
36  @Path("/perfiles")
37  @Produces(MediaType.APPLICATION_JSON)
38  public ArrayList<PerfilDTO> getTodosPerfiles() throws Exception {
39
40      ArrayList<PerfilDTO> listaRet=null;
41
42      try{
43          listaRet = service.buscaTodosPerfiles();
44      }catch(Exception e){
45          e.printStackTrace();
46      }
47      return listaRet;
48  }

```

Listado 3.11 Método para el registro de información del username de X.

```

1  @POST
2  @Path("/perfiles/registrar")
3  @Consumes(MediaType.APPLICATION_FORM_URLENCODED)
4  public Response registrarPerfil(@QueryParam("txtCurp") String sCurp,
5                                @QueryParam("txtPerfil") String sPerfil) throws Exception {
6      @SuppressWarnings("UnusedAssignment")
7      Response response = null;
8
9      try {
10         if (sCurp.isEmpty() && sPerfil.isEmpty()) {
11             response = Response.notAcceptable(null).build();
12         } else {
13             service.registrarPerfil(sCurp, sPerfil);
14             System.out.println(sCurp);
15             response = Response.status(Response.Status.ACCEPTED)
16                             .entity("{\"sSit\":true\"}").build();
17         }
18     } catch (Exception e) {
19         e.printStackTrace();
20         response = Response.serverError().build();
21     }
22     return response;
23 }

```

Listado 3.12 Método para la actualización de información del username de X.

```

1  @PUT
2  @Path("/perfiles/actualizar")
3  @Consumes(MediaType.APPLICATION_FORM_URLENCODED)
4  public Response actualizarPerfil(@QueryParam("txtCurp") String sCurp,
5                                  @QueryParam("txtPerfil") String sPerfil) throws Exception {
6      @SuppressWarnings("UnusedAssignment")
7      Response response = null;
8
9      try {
10         if (sCurp.isEmpty() && sPerfil.isEmpty()) {
11             response = Response.notAcceptable(null).build();
12         } else {
13             service.actualizarPerfil(sCurp, sPerfil);
14
15             System.out.println(sCurp);
16             response = Response.status(Response.Status.ACCEPTED)
17                             .entity("{\"sSit\":true\"}").build();
18         }
19     } catch (Exception e) {
20         e.printStackTrace();
21         response = Response.serverError().build();
22     }
23
24     return response;
25 }

```

3.2.3.7. Pruebas

En esta sección se presentan las pruebas realizadas para comprobar el funcionamiento del módulo de la aplicación móvil.

3.2.3.7.1. Inicio de la aplicación móvil

Ya que el módulo desarrollado es parte de una aplicación móvil base en la que el docente es el actor que interactúa con dicha aplicación, para este caso funcionara de la misma manera, por lo tanto, el docente iniciara sesión con el correo electrónico y la contraseña registrada. La figura 3.28 muestra la pantalla del menú principal de la aplicación. Por otro lado, se muestra la pantalla en la que se visualiza el salón de clases con los alumnos correspondientes a dicho grupo, ya que, será el mismo que será monitoreado en el apartado de ciberacoso.

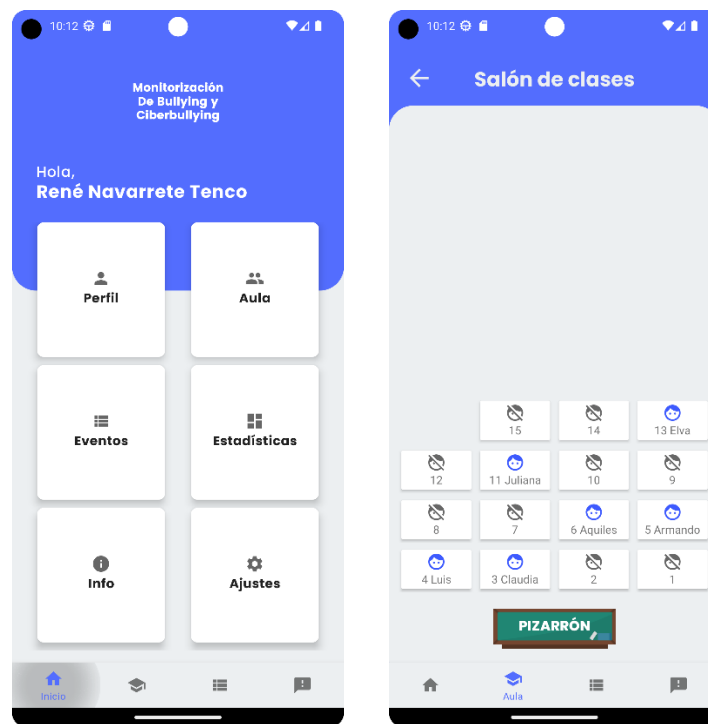


Figura 3.28 Interfaces del menú principal de la aplicación y el salón de clases

3.2.3.7.2. Módulo cyberbullying

En la barra de navegación inferior se encuentra el apartado de “Ciberacoso” a través del cual accede al menú principal de módulo, el cual se muestra en la Figura 3.29.



Figura 3.29 Interfaz del menú principal del módulo de ciberacoso.

En la sección de Grupo se muestran los alumnos registrados que conforman el salón de clases y a través del botón “Gestionar perfil” es posible registrar el *username* del perfil de la red social X del alumno o en dado caso modificarlo (Figura 3.30).

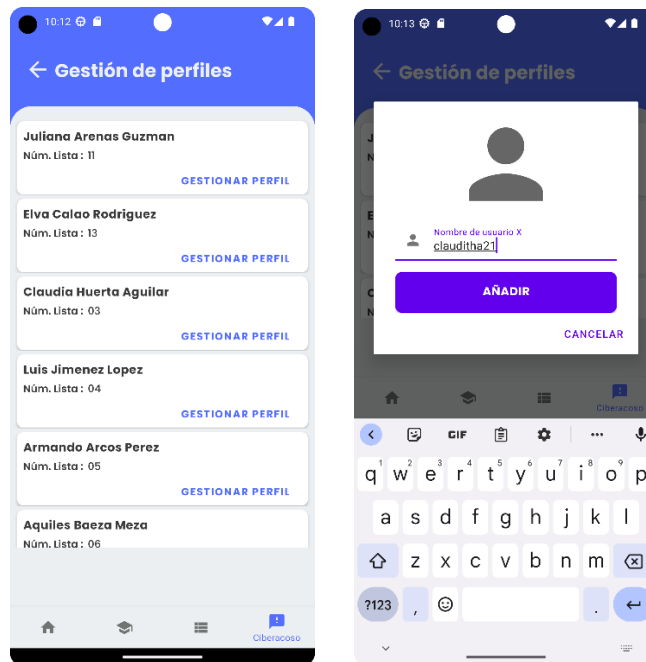


Figura 3.30 Interfaces del listado de alumnos y el registro del perfil de la red social X.

Una vez agregados los perfiles de X, en el apartado de Revisión General se observan todos los tweets emitidos por los alumnos, el texto se torna en rojo si el tweet fue identificado como tweet negativo; por otro lado, la sección de Situaciones de Alerta contiene todos aquellos tweets encontrados como negativos que indiquen posibles indicios de ciberacoso (Figura 3.31).

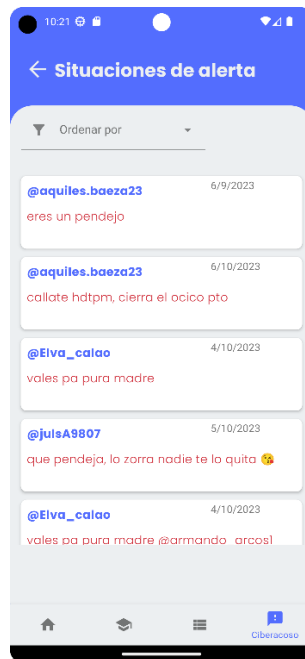


Figura 3.31 Interfaz de las situaciones de alerta.

El docente visualiza las estadísticas obtenidas en el apartado indicado como Dashboard (Figura 3.32), con la posibilidad de observar gráficas, como de pastel que indican la cantidad de tweets negativos y positivos encontrados, los tweets negativos emitidos por alumno y la cantidad de tweets de acuerdo a su clasificación, encontrados en cada semana.

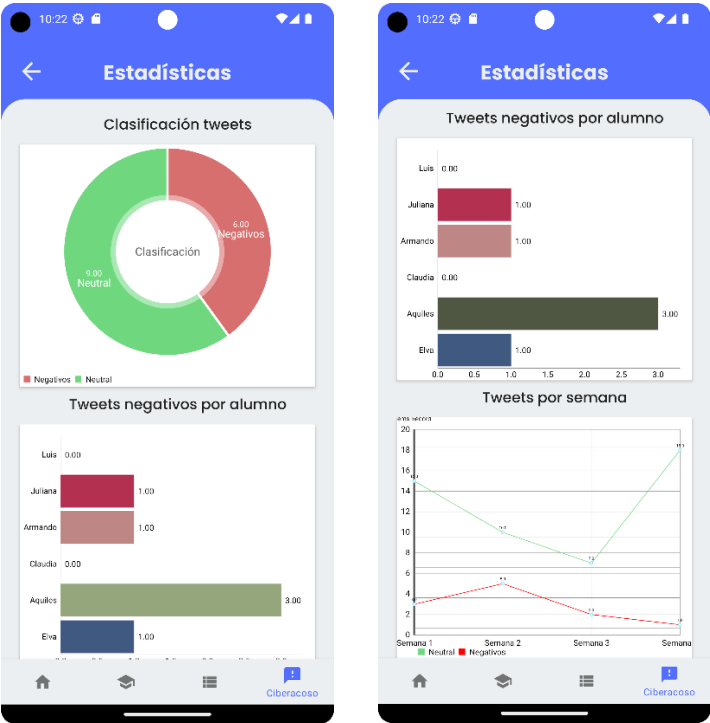


Figura 3.32 Interfaces de la sección de dashboard con las estadísticas.

Capítulo 4. Resultados

A continuación, en este capítulo se describe la valoración por parte de un experto en el área de la psicología y se muestran los resultados obtenidos tras las pruebas realizadas y el panorama que involucra el presente proyecto.

A través del módulo de la aplicación móvil desarrollado, el docente tiene la accesibilidad de monitorizar la presencia de posibles casos de ciberacoso que se encuentren ocurriendo entre los alumnos que contemplan su grupo de clases a través de la red social X; mismo grupo que se monitorea en el módulo de bullying.

4.1. Valoración del módulo de la aplicación móvil

Como se ha mencionado anteriormente, el ciberacoso es un fenómeno en el cual una persona utiliza la tecnología, como internet y las redes sociales, para acosar, intimidar o causar daño a otra persona. En el ámbito comprendido por la psicología, el fenómeno del ciberacoso se considera como una forma específica de comportamiento agresivo que desarrolla consecuencias emocionales y psicológicas significativas para la víctima que sufra de este tipo de acoso.

Una parte fundamental del ciberacoso, es la intervención psicológica; en la que los profesionales de la psicología desempeñan un papel crucial en la intervención y apoyo a las víctimas de ciberacoso. Por ejemplo, el incluir la provisión de asesoramiento para abordar los efectos emocionales y ayudar a desarrollar estrategias de afrontamiento saludables. Por otra parte, también la psicología desempeña un papel en la prevención del ciberacoso, contribuyendo a programas de concienciación y educación; lo que implica trabajar con individuos, comunidades, proyectos y sistemas escolares para fomentar un entorno en línea más seguro.

Debido a que el ciberacoso es un fenómeno que implica agresiones de diversos tipos, es necesario que un experto en el área se involucre en el presente proyecto, con la finalidad de expresar sus opiniones acerca del mismo, observaciones o mejoras que

se incluyen desde su punto de vista profesional. Para ello, se realizó la conexión con la licenciada en psicología Ana Daniela Dávila Carmona, perteneciente al centro psicológico DIPAAM, con ubicación en Apizaco Tlaxcala; con quien se llevó a cabo la tercera parte comprendida para las estancias profesionales.

4.1.1. Retroalimentación

Para llevar a cabo el análisis del módulo de la aplicación móvil, se brindó el contexto explícito a la psicóloga Ana Daniela Dávila Carmona (con cedula profesional 13695368) perteneciente al centro psicológico DIPAAM, explicando la delimitación del proyecto; en donde se hizo hincapié que se pretende detectar posibles casos de ciberbullying a través del análisis de textos, de igual forma se expuso el procedimiento y uso del modelo para realizar la clasificación de los tweets negativos y la funcionalidad general del módulo de la aplicación móvil. Por otro lado, se hizo hincapié, que el foco de la aplicación son las alertas de posibles casos de ciber agresiones, ya que la aplicación no pretende suplantar la atención médica o psicológica de expertos en el área, simplemente detectar anomalías que puedan estar ocurriendo entre los jóvenes a través de la red social (en este caso, X).

Posteriormente, con la ayuda de la psicóloga se plantearon las siguientes observaciones:

“En primer lugar, modificar la denominación de “tweets maliciosos” a “tweets negativos o violentos” que parte de la importancia de erradicar temas con relación a violencia, ya que el ciberbullying forma parte de este, con el objetivo de que el usuario que utilice la aplicación conozca que se estarán abordando aspectos negativos de los cuales debe tener dicho conocimiento.

Como segunda observación se encuentra que es necesario incluir en la sección de las reglas que se clasifiquen como “ciberbullying” aquellos mensajes relacionados con acoso, ya que forma parte importante dentro de dicha problemática, el acoso es un comportamiento que se manifiesta y que abarca aspectos verbales (donde se incluyen

burlas o insultos), sociales y físicos. Ya que si bien es una problemática que permanece de forma latente dentro de redes sociales como twitter; a su vez se incluyen las diversas formas en las que puede persistir la violencia dentro del área académica.”

Gracias a las observaciones realizadas por la psicóloga, se analizaron y atendieron los siguientes puntos:

Como primer punto, al conjunto de reglas de clasificación se agregó una nueva regla, la cual se indica que se clasificaran como ciberacoso aquellos “mensajes que incluyan incentivos de acoso u hostigamiento, ya sea verbal, social o físico”. Dicha regla fue agregada al conjunto previo de reglas de clasificación en la sección de etiqueta ciberbullying (Figura 4.1).

Reglas para etiquetado

La etiqueta o categoría asignada a cada documento es una las siguientes: "Cyberbullying", "No Cyberbullying", "No relacionado", de acuerdo a las siguientes reglas:

- **Cyberbullying.** Un documento es etiquetado en esta categoría si contiene:
 - Por lo menos una grosería dirigida a una persona o varias personas.
 - Mensajes que contengan palabras hirientes dirigidas a una o varias personas.
 - Mensajes que inciten a la discriminación.
 - Mensajes que insulten a una persona o varias personas.
 - Mensajes que amenacen a una persona o varias personas.
 - Mensajes que denigren a un sexo en específico.
 - Maldiciones o burlas en contra de una persona o varias personas.
 - Mensajes que tengan como objetivo ridiculizar a una persona o varias personas.
 - Mensajes que contengan un apodo despectivo hacia un individuo o individuos.
 - **Mensajes que incluyan incentivos de acoso u hostigamiento (verbal, social o físico).**
 - Mensajes que contengan emojis relacionados con el ciberacoso

- **No Cyberbullying.** Un documento se considera en esta categoría si al leerse se identifican:
 - Mensajes que contengan una o varias groserías que no estén dirigidas hacia ninguna persona.
 - Mensajes que adulen a una o varias personas.
 - Mensajes que demuestren apoyo hacia una o varias personas.
 - Mensajes cuya finalidad sea alentar o animar a uno o varios individuos.
 - Mensajes que tengan como objetivo defenderse o defender a otra/as personas; sin intención de insultar.
- **No relacionado.** Un documento se etiqueta como no relacionado si contiene:
 - Mensajes que no tengan relación con los puntos anteriores, como noticias, campañas de marketing o publicidad.
 - Mensajes donde únicamente coloquen hashtags o se etiqueten personas
 - Mensajes que realicen invitaciones a conferencias, concursos, programas de radio, entre otros.
 - Mensajes que contengan imágenes o enlaces.

Figura 4.1 Regla añadida al conjunto previo de reglas.

Se realizó una revisión al conjunto de datos y no se presentaron anomalías, ya que de igual forma algunos mensajes que contenían algún incentivo de acoso en su mayoría se veían acompañados de blasfemias o lenguaje ofensivo.

Y por último, atendiendo a la segunda observación se determinó que la denominación a los tweets que contuvieran lenguaje ofensivo o sean identificados con posible indicio de ciberacoso, se denominen "Tweets negativos".

Una vez atendidas las observaciones, la psicóloga brindó su retroalimentación profesional, la cual se describe explícitamente a continuación:

“Una vez realizada la revisión a dicho módulo hago conocimiento de que se han realizado las modificaciones pertinentes y que a su vez corresponden y cubren con las necesidades de dicha problemática. De igual forma hago mención de que el trabajo de tesis cuenta con los lineamientos correspondientes a abordar el tema de ciberbullying, ya que existe un manejo del tema, el abordaje de la problemática y a su vez existe la identificación de factores de riesgo que persisten dentro de redes sociales y a los cuales están expuestos los alumnos.

La propuesta para la identificación de ciberbullying me resulta innovadora, eficaz y confiable, es una excelente propuesta a implementar dentro de las aulas.”

- Psic. Ana Daniela Dávila Carmona

4.2. Monitorización de posibles casos de ciberacoso

Ya que el presente proyecto es un módulo de una aplicación móvil base que monitoriza eventos de bullying en un salón de clases, se pretende que la detección de las posibles situaciones de ciberacoso sea en torno al grupo de alumnos que lidera el docente en cuestión. Sin embargo, ya que el principal objetivo del módulo de la aplicación es la detección de posibles situaciones de ciberacoso aplicado a la red social X, es posible

realizar la detección de los tweets negativos de cualquier cuenta/perfil de dicha plataforma.

Por lo tanto, el escenario planteado contempla 5 perfiles de la red social X para el análisis de los tweets posteados y su correspondiente clasificación. Planteando dos escenarios, en los que se detectan tweets negativos y tweets en calidad de positivos (esto incluye tweets clasificados en no ciberbullying y en no relacionado).

Previsualización de tweets a clasificar (Figura 4.2):





Vamos que si se puede, somos más y más unidos ❤️❤️❤️

Figura 4.2 Conjunto de tweets para su clasificación.

4.2.1. Resultados de las pruebas

Para comprobar el funcionamiento de la clasificación de los diferentes tweets, los perfiles fueron agregados a través de la aplicación móvil y fueron enlazados a datos de estudiantes.

En la sección de Grupo, se contempla la lista de los estudiantes almacenados, en este caso se contemplan 5 estudiantes listados. Seleccionando el botón de Gestionar perfil se despliega la ventana correspondiente para agregar el perfil de la red social X (Figura 4.3).

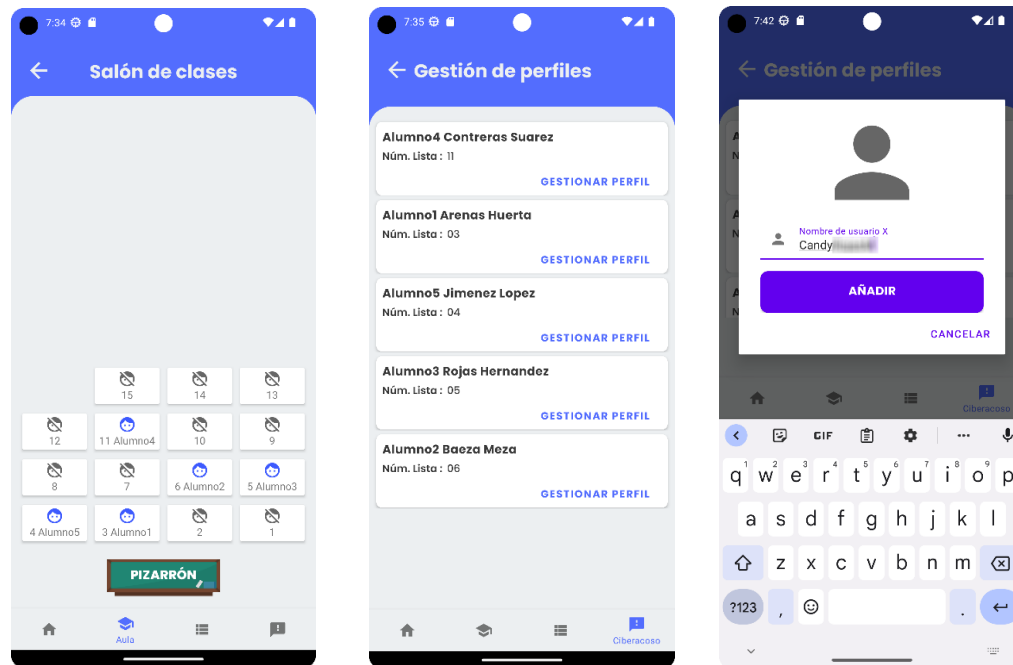


Figura 4.3 Alumnos contemplados y el registro del perfil de la red social X.

En la sección Revisión general (Figura 4.4) el docente a cargo observa los tweets emitidos por los diferentes perfiles (últimos tweets realizados). Y en la sección Situaciones de alerta se mostrarán los tweets negativos catalogados como cyberbullying, de tal manera que sea más intuitivo y visual para el docente.

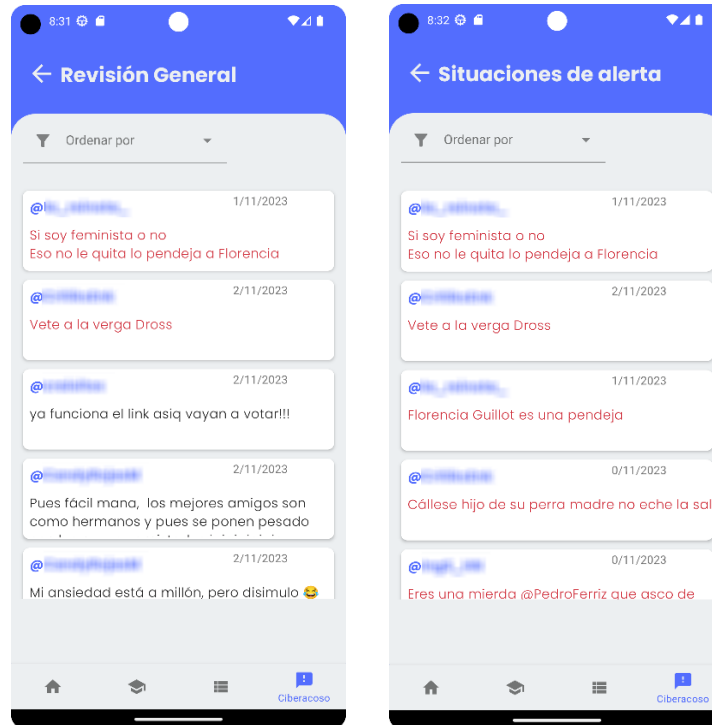


Figura 4.4 Visualización de tweets negativos y positivos o neutrales.

4.3. Evaluación y resultados

La clasificación de los tweets analizados se muestra en referencia a un semáforo con dos estados, color rojo para contemplar aquellos tweets negativos (Figura 4.5) y color verde que indica que los tweets son neutrales o en calidad de positivos (Figura 4.6); por lo tanto, la clasificación concluyo de la siguiente manera:



Tweets identificados como negativos:

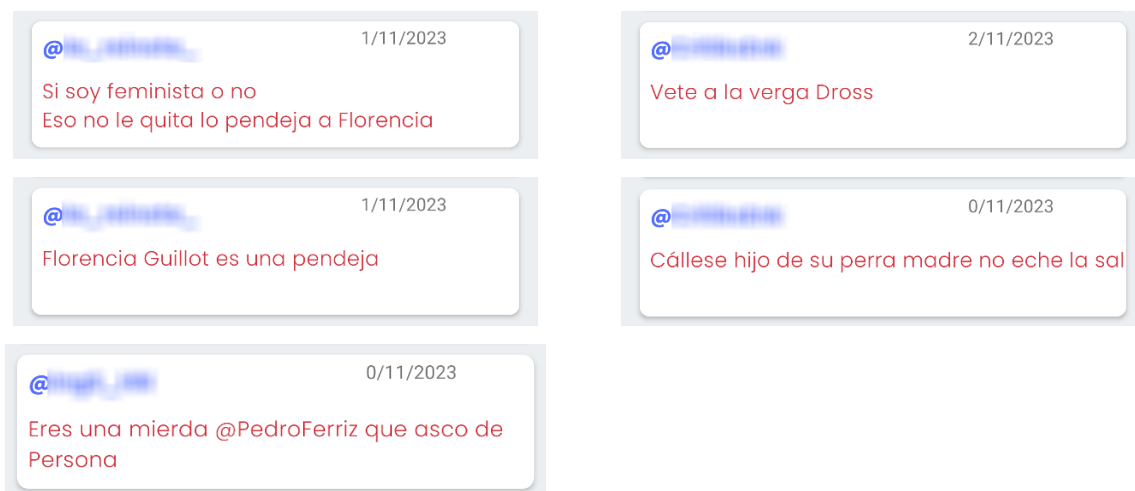


Figura 4.5 Tweets clasificados como negativos.



Tweets identificados como neutrales o en calidad de positivos:



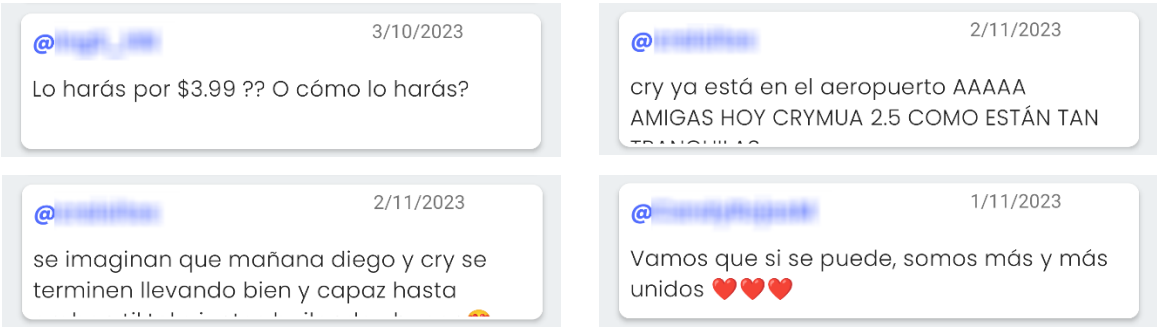


Figura 4.6 Tweets clasificados como neutrales o en calidad de positivos.

De igual forma se muestra en la sección de Dashboard (Figura 4.7), las estadísticas que se obtuvieron a partir de los datos analizados; permitiendo que el docente visualice un reporte gráfico.

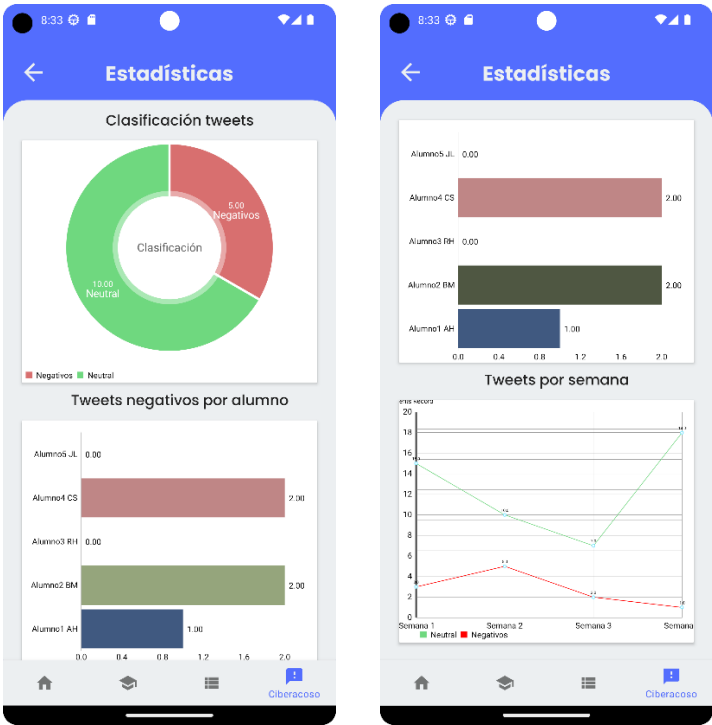


Figura 4.7 Estadísticas de la clasificación.

Capítulo 5. Conclusiones y recomendaciones

5.1. Conclusiones

A pesar que el fenómeno de cyberbullying no es algo nuevo, tiene un aumento considerable en los últimos años, ya que los adolescentes se encuentran más presentes en las redes sociales y a su vez más expuestos a sufrir algún tipo de acoso. Aunque se han implementado medidas para prevenir el bullying y cyberbullying, regularmente de manera informativa; existen pocas soluciones que detecten y prevengan alguna situación de cyberbullying. Actualmente existen métodos que permiten clasificar mensajes ofensivos; sin embargo, la mayoría están enfocados a otros idiomas lo que conlleva que el lenguaje sea diferente al español, cambiando también las palabras o términos que se suelen usar para ofender o humillar a una persona. Debido a lo anterior, el módulo desarrollado en este proyecto, cumple con su principal objetivo, el cual es detectar posibles situaciones de ciberbullying empleando procesamiento de lenguaje natural y a través de algoritmos de aprendizaje supervisado; lo que permite la detección de tweets o posts negativos aplicado en la red social X.

La valoración por parte de una persona involucrada en el área profesional de la psicología permitió contemplar aspectos importantes sobre el estudio en cuestión que apoyaron con el desarrollo del módulo de la aplicación móvil; y su posterior aprobación en base a una opinión profesional.

5.2. Recomendaciones

Como se analizó anteriormente, la problemática del ciberacoso contempla muchos factores, pues es un fenómeno que se manifiesta de diversas maneras en el entorno virtual que contemplan las redes sociales; es por ello que como algún proyecto a futuro se contemple la identificación de estas agresiones en diversos medios o a través de diferentes manifestaciones, si bien la principal manera de comunicación en las redes

sociales es por medio de textos, también se presentan mensajes o frases en imágenes, donde algunas de estas algunas veces son empleadas con propósito de ofensa o agresión.

Por otra parte, aunque el proyecto resultante permita identificar mensajes negativos u ofensivos, es importante mencionar que el seguimiento a casos de agresiones es recomendable que se siga de la mano junto a un profesional del área de la salud, para este caso, el área de la salud mental. Pues de acuerdo a las investigaciones realizadas, tanto ser la víctima y ser el personaje agresor trae severas consecuencias que siempre serán preferente sean atendidas a su debido tiempo. Por ello también se recomienda que, padres de familia y docentes se involucren en la concientización de este fenómeno, para que exista una buena educación y un entorno más agradable a través del medio virtual.

Bibliografía

- [1] A. E. , & C. G. B. Kazdin, *Conducta antisocial: evaluación, tratamiento y prevención en la infancia y adolescencia*. Madrir: Piramide, 2002.
- [2] Gozaini O., *Formas Alternativas para la Resolución de Conflictos*. Argentina: Depalma.
- [3] E. Bausela Herreras, “Estrategias para prevenir el bullying en las aulas”, *Interv Psicosoc*, vol. 17, pp. 369–370, 2008.
- [4] Y. de Vas, “Acoso escolar”, *Evidencia, actualizacion en la práctica ambulatoria*, vol. 16, núm. 1, dic. 2013, doi: 10.51987/evidencia.v16i1.6159.
- [5] M. Abramovay, “Victimización en las escuelas. Ambiente escolar, robos y agresiones físicas”, *Revista Mexicana de Investigación Educativa*, vol. 10, pp. 833–864, jul. 2005, [En línea]. Disponible en: <http://www.redalyc.org/articulo.oa?id=14002611>
- [6] C. B. A., *Victimización por bullying*. 2018.
- [7] C. Ardila, H. Marín, y S. Pardo, “Cyberbullying y Facebook: realidad en la virtualidad”, *Nodos y Nudos*, vol. 4, núm. 37, pp. 43–52, jul. 2014, doi: 10.17227/01224328.3123.
- [8] S. Hinduja y J. Patchin, “Cyberbullying : Identification, Prevention, and Response”, *Cyberbullying Research Center*, vol. October, núm. October, pp. 1–9, 2014, [En línea]. Disponible en: (www.cyberbullying.us)
- [9] P. Snyder, C. Kanich, P. Doerfler, y D. McCoy, “Fifteen minutes of unwanted fame: Detecting and characterizing doxing”, en *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, Association for Computing Machinery, nov. 2017, pp. 432–444. doi: 10.1145/3131365.3131385.
- [10] Y. Xu y P. Trzaskawka, “Towards Descriptive Adequacy of Cyberbullying: Interdisciplinary Studies on Features, Cases and Legislative Concerns of Cyberbullying”, *International Journal for the Semiotics of Law*, vol. 34, núm. 4. Springer Science and Business Media B.V., pp. 929–943, el 1 de septiembre de 2021. doi: 10.1007/s11196-021-09856-4.
- [11] S. Bauman, “Cyberbullying: What counselors need to know”, *Cyberbullying: What counselors need to know*, pp. 204–xiii, 204, ago. 2011, doi: 10.1002/9781119221685.

- [12] M. R. Buxarrais, “Redes sociales y educación”, *Education in the Knowledge Society (EKS)*, vol. 17, núm. 2, pp. 15–20, jul. 2016, doi: 10.14201/eks20161721520.
- [13] L. M. Arboleda, “Servicios WEB: Distribución e integración”, 2004.
- [14] J. Nandigam, V. N. Gudivada, y M. Kalavala, “Semantic Web Services”, 2005.
- [15] B. Kiselev y V. Yakutenko, “An Overview of Massive Open Online Course Platforms: Personalization and Semantic Web Technologies and Standards”, en *Procedia Computer Science*, Elsevier B.V., 2020, pp. 373–379. doi: 10.1016/j.procs.2020.02.232.
- [16] J. M. Aguado, I. J. Martínez, y L. Cañete-Sanz, “Evolutionary trends of digital content in mobile applications”, *Profesional de la Informacion*, vol. 24, núm. 6. El Profesional de la Informacion, pp. 787–796, el 1 de noviembre de 2015. doi: 10.3145/epi.2015.nov.10.
- [17] Valarezo P. M., Honores T. J., Gómez M. A., y Vines S. L., “Comparación de tendencias tecnológicas en aplicaciones web”, pp. 28–49, sep. 2018, doi: <http://dx.doi.org/10.17993/3ctecno.2018.v7n3e27.28-49/>.
- [18] McAfee, “Cyberbullying in Plain Sight”, San Jose, CA, ago. 2022.
- [19] G. Vergara y M. Alicia, “El bullying dentro del salón de clases”, 2014.
- [20] M. Garaigordobil, “Conducta antisocial: conexión con bullying/cyberbullying y estrategias de resolución de conflictos”, *Psychosocial Intervention*, vol. 26, núm. 1, pp. 47–54, abr. 2017, doi: 10.1016/j.psi.2015.12.002.
- [21] J. Ortega-Barón, S. Buelga, M. J. C. Caballero, y E. Torralba, “School Violence and Attitude Toward Authority of Students Perpetrators of Cyberbullying”, *Revista de Psicodidactica*, vol. 22, núm. 1, 2017, doi: 10.1387/RevPsicodidact.16398.
- [22] G. R. Paez, “Assessing Predictors of Cyberbullying Perpetration Among Adolescents: the Influence of Individual Factors, Attachments, and Prior Victimization”, *International Journal of Bullying Prevention*, vol. 2, núm. 2, pp. 149–159, 2020, doi: 10.1007/s42380-019-00025-7.
- [23] O. C. Hang y H. M. Dahlan, “Cyberbullying lexicon for social media”, *International Conference on Research and Innovation in Information Systems, ICRIIS*, vol. December-2, 2019, doi: 10.1109/ICRIIS48246.2019.9073679.
- [24] Noviantho, S. M. Isa, y L. Ashianti, “Cyberbullying classification using text mining”, *Proceedings - 2017 1st International Conference on Informatics and*

- Computational Sciences, ICICoS 2017*, vol. 2018-Janua, pp. 241–245, 2017, doi: 10.1109/ICICOS.2017.8276369.
- [25] A. Upadhyay, A. Chaudhari, Arunesh, S. Ghale, y S. S. Pawar, “Detection and prevention measures for cyberbullying and online grooming”, *Proceedings of the International Conference on Inventive Systems and Control, ICISC 2017*, pp. 1–4, 2017, doi: 10.1109/ICISC.2017.8068605.
 - [26] N. Farag, G. McKee, S. A. El-Seoud, y G. Hassan, “Bullying hurts: A survey on non-supervised techniques for cyber-bullying detection”, *ACM International Conference Proceeding Series*, pp. 85–90, 2019, doi: 10.1145/3328833.3328869.
 - [27] Y. N. Silva, D. L. Hall, y C. Rich, “BullyBlocker: toward an interdisciplinary approach to identify cyberbullying”, *Soc Netw Anal Min*, vol. 8, núm. 1, pp. 1–15, 2018, doi: 10.1007/s13278-018-0496-z.
 - [28] A. Akrim y E. Sulasmi, “Student Perception of Cyberbullying in Social Media”, *Talent Development & Excellence*, vol. 12, núm. 1, pp. 322–333, 2020, [En línea]. Disponible en: <http://www.iratde.com>
 - [29] S. Salawu, Y. He, y J. Lumsden, “BullStop: A Mobile App for Cyberbullying Prevention”, pp. 70–74, 2021, doi: 10.18653/v1/2020.coling-demos.13.
 - [30] H. F. Neo, C. C. Teo, y J. L. Han Boon, “Mobile edutainment learning approach: #stopbully”, *ACM International Conference Proceeding Series*, pp. 6–10, 2018, doi: 10.1145/3284497.3284500.
 - [31] A. Chakraborty, Y. Zhang, y A. Ramesh, “Understanding Types of Cyberbullying in an Anonymous Messaging Application”, en *The Web Conference 2018 - Companion of the World Wide Web Conference, WWW 2018*, 2018, pp. 1001–1005. doi: 10.1145/3184558.3191530.
 - [32] S. Kaiser, M. Martinussen, F. Adolfsen, K. Breivik, y H. Kyrrestad, “An app-based intervention for adolescents exposed to cyberbullying in norway: Protocol for a randomized controlled trial”, *JMIR Res Protoc*, vol. 10, núm. 11, 2021, doi: 10.2196/31789.
 - [33] E. R. Kutok *et al.*, “A cyberbullying media-based prevention intervention for adolescents on instagram: Pilot randomized controlled trial”, *JMIR Ment Health*, vol. 8, núm. 9, 2021, doi: 10.2196/26029.

- [34] Y. J. Foong y M. Oussalah, “Cyberbullying system detection and analysis”, *Proceedings - 2017 European Intelligence and Security Informatics Conference, EISIC 2017*, vol. 2017-Janua, pp. 40–46, 2017, doi: 10.1109/EISIC.2017.43.
- [35] L. J. Thun, P. L. Teh, y C. Bin Cheng, “CyberAid: Are your children safe from cyberbullying?”, *Journal of King Saud University - Computer and Information Sciences*, vol. 34, núm. 7, pp. 4099–4108, 2021, doi: 10.1016/j.jksuci.2021.03.001.
- [36] M. M. Singh, P. J. Ng, K. M. Yap, M. H. Husin, y N. H. A. H. Malim, “Cyberbullying and a mobile game app? An initial perspective on an alternative solution”, *Journal of Information Processing Systems*, vol. 13, núm. 3, pp. 559–572, 2017, doi: 10.3745/JIPS.04.0033.
- [37] E. Olca y O. Can, “Extending FOAF and Relationship Ontologies with Consent Ontology”, *UBMK 2018 - 3rd International Conference on Computer Science and Engineering*, pp. 542–546, 2018, doi: 10.1109/UBMK.2018.8566297.
- [38] M. R. P. Hernandez, L. A. R. Hernandez, C. R. Torres, G. P. Camarena, y B. A. O. Zepahua, “Resource Description Framework and Friend of A Friend-Based Web and Mobile Applications Prototype in an Education Environment A real-time management of students academic profiles”, *Proceedings - 2019 7th International Conference in Software Engineering Research and Innovation, CONISOFT 2019*, pp. 201–206, 2019, doi: 10.1109/CONISOFT.2019.00036.
- [39] O. Thinnukool, P. Khuwuthyakorn, y R. Sittichai, “The Use of Cyberbullying Mobile Application to Increase Perceived Knowledge of Cyberbullying among Adolescents”, *International Journal of Innovation and Technology Management*, vol. 15, núm. 3, pp. 1–19, 2018, doi: 10.1142/S0219877018500293.
- [40] Microsoft, “Información general sobre ASP.NET MVC”. Consultado: el 28 de julio de 2022. [En línea]. Disponible en: <https://docs.microsoft.com/es-es/aspnet/mvc/overview/older-versions-1/overview/asp-net-mvc-overview>
- [41] R. Baxter, N. Hastings, A. Law, y E. J. . Glass, *Java programing (eBook)*, 7a ed., vol. 39, núm. 5. McGraw Hill Professional, 2008.
- [42] Inc. Eclipse Foundation, “Eclipse Jersey”. Consultado: el 21 de julio de 2022. [En línea]. Disponible en: <https://eclipse-ee4j.github.io/jersey/>
- [43] The Apache Software Foundation, “Apache NetBeans”. Consultado: el 21 de julio de 2022. [En línea]. Disponible en: <https://netbeans.apache.org/>

- [44] “Android Studio. Introducción a Android Studio”. Consultado: el 21 de julio de 2022. [En línea]. Disponible en: <https://developer.android.com/studio/intro>
- [45] The Apache Software Foundation, “Apache Jena Fuseki”. Consultado: el 1 de octubre de 2022. [En línea]. Disponible en: <https://jena.apache.org/documentation/fuseki2/>
- [46] Google, “Android. ¿Qué es Android?” Consultado: el 21 de julio de 2022. [En línea]. Disponible en: https://www.android.com/intl/es-419_mx/what-is-android/
- [47] P. Abrahamsson *et al.*, “Mobile-D: An agile approach for mobile application development”, en *Proceedings of the Conference on Object-Oriented Programming Systems, Languages, and Applications, OOPSLA*, 2004, pp. 174–175. doi: 10.1145/1028664.1028736.
- [48] The Apache Software Foundation, “Welcome to Apache OpenNLP”. Consultado: el 22 de julio de 2022. [En línea]. Disponible en: <https://opennlp.apache.org/>
- [49] NLTK Project, “Natural Language Toolkit: Documentation”. [En línea]. Disponible en: <https://www.nltk.org/>
- [50] Stanford NLP Group, “CoreNLP”. Consultado: el 22 de julio de 2022. [En línea]. Disponible en: <https://stanfordnlp.github.io/CoreNLP/>
- [51] John Snow Labs Inc., “Spark NLP”. Consultado: el 22 de julio de 2022. [En línea]. Disponible en: <https://nlp.johnsnowlabs.com/>
- [52] R. P. Ang, “Adolescent cyberbullying: A review of characteristics, prevention and intervention strategies”, *Aggress Violent Behav*, vol. 25, pp. 35–42, 2015, doi: 10.1016/j.avb.2015.07.011.
- [53] L. Christian Elledge, A. Williford, A. J. Boulton, K. J. DePaolis, T. D. Little, y C. Salmivalli, “Individual and Contextual Predictors of Cyberbullying: The Influence of Children’s Provictim Attitudes and Teachers’ Ability to Intervene”, *J Youth Adolesc*, vol. 42, núm. 5, pp. 698–710, 2013, doi: 10.1007/s10964-013-9920-x.
- [54] R. Slonje, P. K. Smith, y A. Frisén, “The nature of cyberbullying, and strategies for prevention”, *Comput Human Behav*, vol. 29, núm. 1, pp. 26–32, 2013, doi: 10.1016/j.chb.2012.05.024.
- [55] INEGI, “Módulo sobre ciberacoso, Comunicado de prensa num. 364, el 13 de julio de 2022”, 2022. [En línea]. Disponible en: <https://www.inegi.org.mx/programas/mociba/2021/>

- [56] V. Balakrishnan, "Cyberbullying among young adults in Malaysia: The roles of gender, age and Internet frequency", *Comput Human Behav*, vol. 46, pp. 149–157, 2015, doi: 10.1016/j.chb.2015.01.021.
- [57] D. P. F. Izabela Zych, Anna C. Baldry, "School Bullying and Cyberbullying: Prevalence, Characteristics, Outcomes, and Prevention", *Handbook of Behavioral Criminology*, núm. 2012, pp. 1–762, 2018, doi: 10.1007/978-3-319-61625-4.
- [58] T. E. Waasdorp y C. P. Bradshaw, "The overlap between cyberbullying and traditional bullying", *Journal of Adolescent Health*, vol. 56, núm. 5, pp. 483–488, 2015, doi: 10.1016/j.jadohealth.2014.12.002.
- [59] L. T. McLoughlin, "Understanding and measuring coping with cyberbullying in adolescents: exploratory factor analysis of the brief coping orientation to problems experienced inventory", *Current Psychology*, vol. 40, núm. 9, pp. 4300–4310, 2021, doi: 10.1007/s12144-019-00378-8.
- [60] R. M. Kowalski y S. P. Limber, "Electronic Bullying Among Middle School Students", *Journal of Adolescent Health*, vol. 41, núm. 6 SUPPL., pp. 22–30, 2007, doi: 10.1016/j.jadohealth.2007.08.017.
- [61] Bill Belsey, "Cyberbullying: An Emerging Threat To The 'Always On' Generation", Bill Belsey, Category: Cyberbullying. [En línea]. Disponible en: <https://billbelsey.com/?cat=13>
- [62] P. Redmond, J. v. Lock, y V. Smart, "Developing a cyberbullying conceptual framework for educators", *Technol Soc*, vol. 60, núm. October, p. 101223, 2020, doi: 10.1016/j.techsoc.2019.101223.
- [63] T. Toshack y S. Colmar, "A cyberbullying intervention with primary-aged students", *Australian Journal of Guidance and Counselling*, vol. 22, núm. 2, pp. 268–278, 2012, doi: 10.1017/jgc.2012.31.
- [64] J. J. Dooley, J. Pyzalski, y D. Cross, "Cyberbullying versus face-to-face bullying: A theoretical and conceptual review", *Journal of Psychology*, vol. 217, núm. 4, pp. 182–188, 2009, doi: 10.1027/0044-3409.217.4.182.
- [65] R. M. Kowalski y S. P. Limber, "Psychological, physical, and academic correlates of cyberbullying and traditional bullying", *Journal of Adolescent Health*, vol. 53, núm. 1 SUPPL., pp. S13–S20, 2013, doi: 10.1016/j.jadohealth.2012.09.018.

- [66] R. A. Sabella, J. W. Patchin, y S. Hinduja, “Cyberbullying myths and realities”, *Comput Human Behav*, vol. 29, núm. 6, pp. 2703–2711, 2013, doi: 10.1016/j.chb.2013.06.040.
- [67] INEGI, “Módulo sobre Ciberacoso 2019”. [En línea]. Disponible en: <https://www.inegi.org.mx/rnm/index.php/catalog/589>
- [68] INEGI, “COMUNICADO DE PRENSA NÚM . 208 / 18 16 DE MAYO DE 2018 ‘ Estadísticas a propósito del día Mundial del Internet (17 de Mayo)’ Datos Nacionales.”, pp. 1–8, 2022, [En línea]. Disponible en: <https://www.inegi.org.mx/programas/dutih/2019/>
- [69] G. García-Maldonado, V. M. Joffre-Velázquez, G. J. Martínez-Salazar, y A. Llanes-Castillo, “Cyberbullying: forma virtual de intimidación escolar”, *Rev Colomb Psiquiatr*, vol. 40, núm. 1, pp. 115–130, 2011, doi: 10.1016/s0034-7450(14)60108-6.
- [70] J. S. Chun, J. Lee, J. Kim, y S. Lee, “An international systematic review of cyberbullying measurements”, *Comput Human Behav*, vol. 113, núm. July, p. 106485, 2020, doi: 10.1016/j.chb.2020.106485.
- [71] P. K. Smith, *Narratives in Research and Interventions on Cyberbullying among Young People*. Springer International Publishing, 2019. doi: 10.1007/978-3-030-04960-7.
- [72] H. Vandebosch y K. van Cleemput, “Cyberbullying among youngsters: Profiles of bullies and victims”, *New Media Soc*, vol. 11, núm. 8, pp. 1349–1371, 2009, doi: 10.1177/1461444809341263.
- [73] P. K. Smith, J. Mahdavi, M. Carvalho, S. Fisher, S. Russell, y N. Tippett, “Cyberbullying: Its nature and impact in secondary school pupils”, *J Child Psychol Psychiatry*, vol. 49, núm. 4, pp. 376–385, 2008, doi: 10.1111/j.1469-7610.2007.01846.x.
- [74] S. Hinduja y J. W. Patchin, “Cyberbullying: An exploratory analysis of factors related to offending and victimization”, *Deviant Behav*, vol. 29, núm. 2, pp. 129–156, 2008, doi: 10.1080/01639620701457816.
- [75] P. Corona, “¿Qué es el cyberbullying?” [En línea]. Disponible en: <https://www.gob.mx/ciberbullying/articulos/que-es-el-ciberbullying>
- [76] D. Mariana, B. Tarigan, L. Riwu, y S. Monika, “Use of Cyberbullying Language on Instagram Social Media”, vol. 01047, 2022.

- [77] K. Kopecký, “Cyberbullying and Other Risks of Internet Communication Focused on University Students”, *Procedia Soc Behav Sci*, vol. 112, núm. Iccpsy 2013, pp. 260–269, 2014, doi: 10.1016/j.sbspro.2014.01.1163.
- [78] B. Nieto, I. Portela, E. López, y V. Domínguez, “Verbal violence in students of compulsory secondary education.”, *Eur J Investig Health Psychol Educ*, vol. 8, núm. 1, pp. 5–14, 2018, doi: 10.30552/ejihpe.v8i1.221.
- [79] Y. Xu, “The Invisible Aggressive Fist: Features of Cyberbullying Language in China”, *International Journal for the Semiotics of Law*, vol. 34, núm. 4, pp. 1041–1064, 2021, doi: 10.1007/s11196-020-09746-1.
- [80] J. A. Martínez Lara, “Los insultos y palabras tabúes en las interacciones juveniles. Un estudio sociopragmático funcional”, *Boletín de Lingüística*, vol. 21, núm. 31, 2009.
- [81] Ministerio de educación, “Ciberacoso en 100 palabras”, Hay palabras que matan. [En línea]. Disponible en: <https://www.mineduc.cl/ciberacoso/>
- [82] A. Alipan, J. L. Skues, S. Theiler, y L. Wise, “Defining Cyberbullying: a Multifaceted Definition Based on the Perspectives of Emerging Adults”, *International Journal of Bullying Prevention*, vol. 2, núm. 2, pp. 79–92, 2020, doi: 10.1007/s42380-019-00018-6.
- [83] D. Álvarez-García, A. Barreiro-Collazo, J. C. Núñez, y A. Dobarro, “Validity and reliability of the Cyber-aggression Questionnaire for Adolescents (CYBA)”, *European Journal of Psychology Applied to Legal Context*, vol. 8, núm. 2, pp. 69–77, 2016, doi: 10.1016/j.ejpal.2016.02.003.
- [84] S. Buelga, B. Martínez-Ferrer, M. J. Cava, y J. Ortega-Barón, “Psychometric properties of the CYBVICS cyber-victimization scale and its relationship with psychosocial variables”, *Soc Sci*, vol. 8, núm. 1, 2019, doi: 10.3390/socsci8010013.
- [85] S. Buelga, J. Postigo, B. Martínez-Ferrer, M. J. Cava, y J. Ortega-Barón, “Cyberbullying among adolescents: Psychometric properties of the CYB-AGS cyber-aggressor scale”, *Int J Environ Res Public Health*, vol. 17, núm. 9, 2020, doi: 10.3390/ijerph17093090.
- [86] H. Brighi, A., Ortega, R., Pyzalski, J., Scheithauer, H., Smith, P. K., Tsormpatzoudis, H., Tsorbatzoudis, “European Cyberbullying Intervention Project Questionnaire (ECIPQ)”, *APA PsycTests*, 2012, doi: 10.1037/t66195-000.

- [87] J. M. González-Cabrera, A. León-Mejía, J. M. Machimbarrena, A. Balea, y E. Calvete, “Psychometric properties of the cyberbullying triangulation questionnaire: A prevalence analysis through seven roles”, *Scand J Psychol*, vol. 60, núm. 2, pp. 160–168, 2019, doi: 10.1111/sjop.12518.
- [88] E. Calvete, I. Orue, A. Estévez, L. Villardón, y P. Padilla, “Cyberbullying in adolescents: Modalities and aggressors’ profile”, *Comput Human Behav*, vol. 26, núm. 5, pp. 1128–1135, 2010, doi: 10.1016/j.chb.2010.03.017.
- [89] S. Berne *et al.*, “Cyberbullying assessment instruments: A systematic review”, *Aggress Violent Behav*, vol. 18, núm. 2, pp. 320–334, 2013, doi: 10.1016/j.avb.2012.11.022.
- [90] T. Pozzoli y G. Gini, “Behavior during cyberbullying episodes: Initial validation of a new self-report scale”, *Scand J Psychol*, vol. 61, núm. 1, pp. 22–29, 2020, doi: 10.1111/sjop.12517.
- [91] BCNRESOL ODR SOLUTIONS SL, “b-resol”. [En línea]. Disponible en: <https://b-resol.com/>
- [92] ReThink Inc., “ReThink”. [En línea]. Disponible en: <https://www.rethinkwords.com/>
- [93] Grupo DAS, “DAS”, Nuestras Apps. Proofup. [En línea]. Disponible en: <https://www.das.es/apps/>
- [94] SafeToNet Inc., “SafeToNet”. [En línea]. Disponible en: <https://safetonet.com/>
- [95] ATLAS.ti, “ATLAS.ti”. [En línea]. Disponible en: <https://atlasti.com/es>